FEDERAL EMERGENCY MANAGEMENT AGENCY

INFORMATION TECHNOLOGY ARCHITECTURE

VERSION 2.0

THE ROAD TO e-FEMA

VOLUME I

MAY 2001

FEDERAL EMERGENCY MANAGEMENT AGENCY

INFORMATION TECHNOLOGY ARCHITECTURE

VERSION 2.0

THE ROAD TO e-FEMA

VOLUME I

MAY 2001

Prepared by:

Federal Emergency Management Agency

Information Technology Services (ITS) Directorate

500 C Street, S.W.

Washington, DC 20472

TABLE OF CONTENTS

List of Figures

List of Tables

FOREWORD

THIS DOCUMENT IS the Federal Emergency Management Agency's (FEMA) Version 2.0 of the *Information Technology (IT) Architecture* prepared under *the Information Technology Management Reform Act (ITMRA),* also known as the *Clinger-Cohen Act of 1996,* with the supporting guidance of Office of Management and Budget (OMB) Memorandum M-97-16. This document complies with revised OMB Circular No. A-130 dated November 28, 2000, which incorporates earlier OMB guidance that this document was based upon. This document is an update from Version 1.0 of the initial *FEMA Information Technology Architecture*, published November 2, 1998. This document discusses the progress FEMA has made in implementing its Information Technology Architecture. It also discusses FEMA's implementation of electronic government and how this translates into the Agency becoming e-FEMA.

The *FEMA IT Architecture* is written to be primarily directive in nature to identify and define common high-level IT architectural standards and components that can be applied to all FEMA systems. This document identifies FEMA's Target Architecture Capabilities that represent progress toward reaching the Agency's target architecture depicted in this volume.

Assumptions and Constraints

The following are the basic assumptions and constraints:

- **Continuity, Contingency, and Disaster Recovery Planning.** FEMA has fully complied with PDD-67 on Continuity of Operations Planning (COOP). A separate COOP document is maintained by the Agency. FEMA is also keenly aware of the need to conduct Business Continuity and Contingency Planning (BCCP) for all its core business processes. A considerable BCCP baseline was established, as a result of the Agency's Y2K efforts. This baseline will be updated for ongoing BCCP activities. FEMA is also aware of the need to develop and document formal Disaster Recovery Plans (DRPs) for all its major systems and applications. The Agency will follow all the appropriate guidance to ensure effective DRPs are developed and documented. All of these above contingency planning activities will integrate the appropriate sections of this IT architecture.

- **Unclassified Operations Only.** To make this document accessible to the widest possible audience, the initial *FEMA IT Architecture* was developed and defined for unclassified operations only. Version 2.0 remains unclassified in nature. It is anticipated that future revisions to the *FEMA IT Architecture* will have a classified annex. In related activity, FEMA is developing plans, policies, and security architecture components in response to the Critical Infrastructure Protection (CIP) Program under Presidential Decision Directive 63 (PDD-63).

- **Status of Business Function Allocation.** In developing the *FEMA IT Architecture*, over 500 highly detailed FEMA business functions for FEMA's Directorates and Administrations, Divisions, and Branches currently documented in FEMA's *Missions and Functions Manual* were reviewed and considered. Nearly all of the business functions were determined to be IT-significant to some degree.

- **A Snapshot in Time.** Considering the Presidential transition that occurred on January 20, 2001, the Federal government has a new Administration. Within FEMA, improvement efforts and re-organization are expected to occur. The organization chart and specific discussion of

missions depicted in this document are now subject to change. Version 2.0 of the *FEMA IT Architecture* will be updated as reorganizations of various parts of the Agency occur or as business processes in the Agency are re-engineered. Version 2.0 of the *FEMA IT Architecture* will encourage the enterprise-wide adoption of common architectural components, wherever possible. It sets the stage for the continued development of an integrated IT investment strategy with detailed cost/benefit analyses for selected procurements.

- **Large Requirement for Enterprise Information Flow and Many Program-Centric Systems.** Another important consideration in the development of the initial Version 1.0 and the updated Version 2.0 of the *FEMA IT Architecture* is that over 100 FEMA organizational entities have business associations with well over 200 other external agencies, activities, and partners. Most of these interactions were also determined to be IT significant. Further complicating the analysis was the identification of a comparatively large number of standalone program-centric legacy systems and document and data stores within the various FEMA groups. These legacy systems and document/data stores present challenges for future enterprise-wide IT integration. The analysis clearly pointed to the need for universally accepted standards to achieve information exchange and interoperability among heterogeneous systems.

- **OMB Circular No. A-130, "Management of Federal Information Resources," Revised November 28, 2000.** This revision modifies sections of the Circular concerning information systems and technology management to follow more closely provisions of the *Clinger-Cohen Act* and OMB Circular A-11. This Circular rescinds, among other Directives, OMB Memoranda M-96-20, "Implementation of the Information Technology Management Reform Act of 1996;" M-97-02, "Funding Information Systems Investments;" and M-97-16, "Information Technology Architecture." Version 1.0 and Version 2.0 of the *FEMA IT Architecture* were directly based upon the requirements contained in M-96-20 and M-97-16. The revised Circular now incorporates the provisions of the rescinded Directives. Version 2.0 of the updated *FEMA IT Architecture* was completed prior to the publication date of the revised A-130. However, a review of the revised Circular was made to ensure that this updated *FEMA IT Architecture* is compliant. Throughout this document, the term *IT Architecture* correlates to the new term, *Enterprise Architecture (EA)* in the revised OMB A-130 Directive.

With the large number of IT-significant business functions, associated IT systems and data stores, and internal and external collaborating organizations, the initial Version 1.0 and the updated Version 2.0 of the *FEMA IT Architecture* document address the business functions at a high level. For each business function, FEMA can provide additional supporting details, if required. FEMA has started development of an *FEMA IT Architecture* Data Base to identify and address architecture components for all of the business functions. Future revisions to this document and the development of the ancillary electronic *FEMA IT Architecture* Data Base (described in Section 1.12.1) should help address business functions, information flows, systems/applications, and data stores at progressively finer levels of detail in future revisions to this document.

Use of Terminology

Within the context of the directive tone noted above, the following terms have these meanings:

- The use of the term ***shall*** implies that the statement is mandatory for compliance in the development of future IT systems or for systems that are proposed to be re-engineered. Requests for waivers must be justified and require formal action by the FEMA Information Resources Board (IRB) and the Chief Information Officer (CIO) in accordance with the provisions contained in Section 4 of this document.

- The use of the term ***will*** implies an intent to consider the requirement in earnest in the development of future IT systems or systems that are proposed to be re-engineered. In general, *FEMA IT Architecture* requirements characterized as *will* can be expected to have viable alternatives. In the interest of architectural standardization, proposed systems that do not comply with a *will* requirement must also request a waiver, but the burden-of-proof will not be as stringent.

- The use of the terms ***must***, ***is declared to be***, or ***is determined to be*** should be interpreted in the same sense as the term *shall.*

- The use of the terms ***may***, ***might***, ***could***, ***should*** is intended to be only advisory in nature. At some point in the future, the architectural requirement could be tightened to *will* or *shall* status. There is no requirement to request a waiver or deviation from these standards from the IRB for future IT systems or those proposed to be re-engineered. However, the deviation must be noted in the systems development documentation and must be addressed as appropriate in systems engineering reviews.

Within the Technical Reference Model (Section 2), the following terms have the meanings indicated:

- ***Adopted*** means that the standard or standard tool has been formally accepted by the CIO for the service area or architectural component to which it refers.

- ***Under evaluation*** means that the standard or standard tool has not yet been formally accepted and is being actively evaluated or considered within FEMA.

- ***Suggested*** is a less strong term than *under evaluation*. *Suggested* really means that there is a potential opportunity for technology insertion or standardization that ought to be more formally considered, business case and funding permitting.

- ***In-service use*** means that the standard or tool is currently being used within FEMA IT systems. It is subject to re-evaluation, re-engineering, or additional development prior to being formally adopted.

Mandatory Compliance Statement

This *FEMA IT Architecture* is mandatory for compliance on the development of new IT systems and any proposed re-engineering, re-hosting, or additional development of legacy systems. Section 4 provides amplifying information.

Point of Contact

The point of contact for questions or comments regarding this *FEMA IT Architecture* is G. Clay Hollister, FEMA Chief Information Officer (CIO), at (202) 646-3006. His e-mail address is Clay.Hollister@fema.gov.

1. FEMA ENTERPRISE IT ARCHITECTURE

1.1 INTRODUCTION

This section of the *FEMA IT Architecture* document provides the following:

- Discussion of background, scope, directives, organizations, missions, principles, operational environmental factors, and information technology (IT) management team underlying and supporting the enterprise-wide *FEMA IT Architecture*
- Discussion of high-level FEMA business functions
- High-level information flow requirements and relationships
- Supporting applications and systems
- FEMA document and data descriptions
- Technology infrastructure (e.g., discussion of re-usable IT architectural components).

The complete IT infrastructure and Enterprise Architecture discussed in this section, with all the resulting project integration, depict the road the Agency must follow to become electronic (e-) FEMA. This *FEMA IT Architecture* represents the core foundation for e-FEMA.

Section 2 of this document provides the FEMA Technical Reference Model and standards profiles. Section 3 discusses networking and communications aspects of the *FEMA IT Architecture*. Section 4 addresses maintenance and implementation of the *FEMA IT Architecture*. Volume 2, Appendix P, addresses the Target Architecture Capabilities the Agency has developed, and how these serve as the basis of e-government and e-FEMA.

1.2 BACKGROUND OF ENTERPRISE ARCHITECTURE

FEMA is a small Federal agency with a rather large information flow requirement to support widely-distributed planning and operations with FEMA's numerous business partners and the American public. Within FEMA, IT, networking, and telecommunications resources are widely viewed as being **mission-critical** and **inseparable**.

FEMA did not have a formally defined, enterprise-wide, well-disciplined, and universally accepted IT architecture for development and integration of FEMA IT systems. With the establishment of the FEMA Switched Network (FSN) in 1982 and more recently with the development of the National Emergency Management Information System (NEMIS), FEMA had a rather robust *implied* IT architecture as a *de facto* agency-wide standard. The architectural standard was reflected in such enterprise-wide systems as NEMIS.

With the development and publication of the initial *FEMA IT Architecture, Version 1.0,* in 1998, FEMA formally defined and documented its IT and network technology (NT) architectures. The goal was to achieve more efficiencies and higher levels of integration and interoperability, particularly with other Federal agencies, FEMA's partners, and the American public. This goal was con-

gruent with the *Information Technology Management Reform Act (ITMRA)* as amplified by Office of Management and Budget (OMB) Memorandum, M-97-16, and the revised OMB Circular A-130 dated November 28, 2000, which incorporated earlier guidance. With the passage of the ITMRA and the requirements of revised OMB Circular A-130 dated November 28, 2000, the FEMA Information Technology Services (ITS) Directorate views the development of a formal, enterprise-wide IT architecture as an important and timely opportunity to rigorously define and document the existing FEMA architecture. More important, the ITS Directorate and FEMA senior management also view this as an opportunity to manage FEMA's IT systems development in a more cost-effective, interoperable, scalable, open, standardized, and secure manner in the future. Publication of the updated *FEMA IT Architecture, Version 2.0,* validates the technical rationale that was incorporated in the initial publication.

1.3 DIRECTIVES FOR DEVELOPMENT OF THE *FEMA IT ARCHITECTURE*

The three major standards, policies, and guidelines that apply to this task include:

- ***Clinger-Cohen Act of 1996,* Also Known as the *Information Technology Management Reform Act (ITMRA).*** The ITMRA mandates policies and procedures for agencies to follow in the development and implementation of IT systems, including requirements for inter-agency coordination, technology transfer, performance, and business case analysis. The ITMRA formally established the position of the Chief Information Officer (CIO) within Federal agencies as the focal point for an agency's IT architecture development and management.

- **OMB Memorandum M-97-16, *Information Technology Architectures*, June 18, 1998.** This OMB Memorandum provides guidelines to Federal agencies on the development of their IT architectures to meet the requirements of the ITMRA.

- **OMB Circular No. A-130, Revised November 28, 2000.** This Circular establishes policy for the management of Federal information resources, and includes procedural and analytic guidelines for implementing specific aspects of these policies and appendices. The revision modifies sections of the Circular to follow more closely provisions of the *Clinger-Cohen Act* and OMB Circular A-11. This Circular also rescinds earlier related guidance, such as OMB's M-97-16, by incorporating the same guidance in this Circular.

  FEMA recognizes that decisions on IT architecture must be considered in the light of a number of other mandatory Executive directives, Congressional Acts, and judicial guidance documents. These documents are identified in Appendix I.

1.4 SCOPE AND DEFINITION OF THE FEMA ENTERPRISE AND THE ENTERPRISE IT ARCHITECTURE

The *FEMA Enterprise* is simply and broadly defined to incorporate *all* internal and external resources (including partnerships) needed to accomplish FEMA's mission requirements. These resources include but are not limited to personnel and organizations, Regional Offices and Disaster Field Offices (DFOs), IT resources and services, grant funds, corporate documents and data bases, partnerships with other Federal agencies with their commitments of resources, partnerships with State and local governments, FEMA facilities, fixed and transportable assets, partnerships and associations with voluntary organizations, security and Critical Infrastructure Protection (CIP) resources and measures, telecommunications and networking resources, and other resources that can be impressed into service in the event of a national emergency. Victims of disasters, and sensitivity to their concerns, are also considered an important part of the FEMA enterprise. Management of the FEMA enterprise clearly requires a robust FEMA enterprise IT architecture.

The scope of this *FEMA IT Architecture* covers both IT and NT architectural components. This architecture does so in a seamless fashion because FEMA's mission-critical distributed information flow requirements demand a robust communications and networking backbone. The *FEMA IT Architecture* also broadly includes:

- Business processes
- Information flows (both internal and external)
- Automated and manual interfaces with FEMA partners and victims
- Hardware and software applications
- Documents and data stores
- Historical archives
- Accepted IT standards
- IT research and development resources
- Usable and re-usable components of the National and Global Information Infrastructure (NII/GII)
- IT advances
- Other IT services and resources that can be impressed into service in a national emergency.

Consistent with OMB Capital Planning and Investment Control Process (CPIC) guidance, the *FEMA IT Architecture* provides the ***technology vision*** to guide resource decisions that will reduce costs and improve mission performance. The technology vision is considered within the scope of this *FEMA IT Architecture* document, but the detailed investment strategy and underlying cost/benefit analysis are not. The *FEMA IT Architecture* recognizes that technology and standards recommendations and improvements must be affordable. The *FEMA IT Architecture* sets the stage for cost/benefit analysis in an enterprise environment that is standardized and interoperable. A key presumption is that overall IT enterprise life-cycle costs will be reduced and mission performance will be enhanced through standardization activities. The *FEMA IT Architecture* also sets the stage for FEMA to address Executive Order (EO) 13010 and Presidential Decision Directive 63 (PDD-63) concerned with CIP.

In the development of the Fiscal Year (FY) 2002 budget process, FEMA has taken the initial steps to prepare a comprehensive and tightly integrated IT investment strategy in accordance with OMB Memorandum M-97-02, dated October 25, 1996, entitled *Funding Information Systems Investments.* These steps have resulted in the development of FEMA's first Target Architecture Capabilities that will be considered for funding for FY 2002. OMB's memorandum states: *"Investments in major information systems proposed for funding in the President's budget should be consistent with Federal, agency, and bureau information architectures which: integrate agency work processes and information flows with technology to achieve the agency's strategic goals; and specify standards that enable information exchange and resource sharing."* This *FEMA IT Architecture* provides the required architectural input into the investment strategy process. FEMA is also preparing to publish a separately prepared *Information Technology (IT) Capital Planning and Investment Guide (CPIG),* following OMB's recent update to Circular A-130 on integrating the CPIC with the budget process.

Consistent with PDD-63, FEMA is responsible for protecting its own critical infrastructure especially its cyber-based systems. This is also consistent with the *Computer Security Act.* The CIP directive presents significant IT architectural security challenges. The CIO for FEMA also serves as the Agency's Chief Infrastructure Assurance Officer (CIAO). In November 1998, the CIAO proposed a plan for protecting FEMA's critical infrastructure, which included vulnerability assessments of IT and physical systems as well as recommendations for eliminating significant vulnerabilities. FEMA completed the vulnerability assessments of its major IT systems in October 2000. Further response to the requirements of PDD-63 is a continued matter of high priority for FEMA.

1.5 RELATIONSHIP OF THE *FEMA IT ARCHITECTURE* TO OTHER HIGH-LEVEL DOCUMENTS

FEMA is responsive to public laws, Executive Orders and other Presidential guidance, directives of other agencies (e.g., OMB, General Services Administration [GSA], and the National Archives and Records Administration [NARA]), court decisions, and FEMA's own rules and regulations as published in the *Federal Register* (such as the Code of Federal Regulations (CFR), particularly 44 CFR 1.1). These are listed in Appendices C and I.

From these national-level documents, FEMA has produced FEMA enterprise-level documents that impact the *FEMA IT Architecture* including:

- *FEMA Strategic Plan*
- *Federal Response Plan (FRP)*
- *National Mitigation Strategy*
- *FEMA Annual Performance Plan*
- *Missions and Functions Manual 1010.1*
- *FEMA Information Resource Management Policy and Procedural Directive (FIRMPD)*
- *FEMA IT Capital Planning and Investment Guide (CPIG)*, Draft
- *Government Paperwork Elimination Act (GPEA) Plan.*

1.6 FEMA'S MISSION AND PRINCIPLES

This section refines the scope and coverage of the *FEMA IT Architecture* document and shows that the *FEMA IT Architecture* effectively bridges FEMA's high-level mission requirements with FEMA IT systems.

1.6.1 FEMA Mission Statement

The mission of FEMA is to **reduce the loss of life and property and protect our institutions from all hazards by leading and supporting the Nation in a comprehensive, risk-based emergency management program of mitigation, preparedness, response, and recovery:**

- **Mitigation.** Mitigation is the process of taking sustained actions to reduce or eliminate long-term risk to people and property from hazards and their effects.

- **Preparedness.** Provide the leadership, policy, financial and technical assistance, training, readiness, and exercise support to strengthen (1) community and Tribal readiness through preparedness and (2) the professional infrastructure of trained and tested emergency workers, community leaders, and public citizens who can prepare for disasters, mitigate against disasters, respond to a community's needs after a disaster, and launch an effective recovery effort.

- **Response.** Response is the process of conducting emergency operations to save lives and property by positioning emergency equipment and supplies; evacuating potential victims; providing food, water, shelter, and medical care to those in need; and restoring critical public services.

- **Recovery.** Recovery is the process of rebuilding communities so individuals, businesses, and governments can function on their own, return to normal life, and protect against future hazards.

1.6.2 FEMA Principles of Operation

This section briefly identifies and provides a consolidated listing of FEMA's principles of operation as they relate to design and integration of IT systems. From an IT architecture perspective, these principles provide a set of baseline requirements to be considered in the design, development, and integration of IT systems and networks:

- **Comprehensive Emergency Management (CEM).** The business functions above represent the phases of emergency management and make up what public officials and emergency management professionals refer to as comprehensive emergency management (CEM). FEMA's organization, budget structure, strategic goals, and implementation strategies are directly aligned in support of the Agency's mission and its core business functions. This *FEMA IT Architecture* establishes the baseline and target architecture for IT and NT to support the strategy of CEM. For FEMA, IT represents a strategic resource and an important force multiplier to help support mission-critical business functions across the enterprise.

- **Mitigation as a Cornerstone.** Within FEMA, mitigation is the cornerstone of CEM. Mitigation is an all-hazards-based activity that is widely acknowledged to be IT intensive. Relative to IT systems, mitigation places a premium on intelligent collaboration and visualization along with the concept of creating, managing, using, and disseminating information. The volume of information is large, and the demand for interaction with the information is growing rapidly.

- **Sensitivity to Victims' Concerns.** Sensitivity to the concerns of victims in a disaster is of paramount concern. The major implications for IT systems are that the systems be well-engineered and well-tested. In general, the public has zero tolerance for computer technology that does not work well and in a timely manner, especially during a time of crisis.

- **Quality of Service (QoS).** Required QoS for IT systems and networks is an important design and integration requirement that needs to be addressed in a proactive manner. QoS should not be viewed with a "What you see is what you get" attitude but rather as an opportunity for improvement. Perceptions of poor QoS need to be addressed and resolved.

- **Timeliness and Responsiveness.** IT systems and networks must be designed to improve timeliness and responsiveness of service delivery, not impose delays or impediments to it.

- **Security.** IT systems and network security must be an integral part of the design and engineering process. Within the context of this *FEMA IT Architecture*, the term *security* encompasses document and data integrity, ensured service availability, originator authentication, confidentiality, access controls, non-repudiation, and audit services. Security also encompasses the full scope of plans, policies, procedures, and measures necessary to achieve Continuity of Government (COG), Continuity of Operations (COOP), and Critical Infrastructure Protection (CIP). Requirements for an Enterprise Security Architecture are addressed in Section 2.4.

- **Results-Oriented Business Sense.** The development of IT systems and networks needs to be results-oriented and to make business sense. The FEMA ITS Directorate desires to maximize the effectiveness of its investment portfolio in IT systems. FEMA will report on performance of both IT systems and the IT systems engineering process in accordance with ITMRA, *Government Performance and Results Act (GPRA)*, and customer service requirements.

- **Maximum Leverage of IT, Security, and Telecommunications Resources.** IT systems, security, and telecommunications are resources to be economized just like any other resource (e.g., funding, human resources).

- **Disciplined Approach to IT Systems Development.** Emphasis needs to be placed on designing, developing, and integrating systems and networks in a disciplined manner across the FEMA enterprise. This includes establishment of accepted life-cycle models and enterprise-wide approaches for configuration management and systems engineering.

- **Standards.** To achieve interoperability and portability, IT systems and telecommunications standards are important and make good business sense. FEMA has a firm commitment to implement open systems approaches wherever practicable in coordination with its business partners.

- **Partnerships and Coordination.** In providing comprehensive emergency management, FEMA serves a vital coordination role toward achieving consensus across a significant number of external activities. IT systems and networks need to be designed, developed, and integrated in consideration of the systems for FEMA's business partners, the Regions, the States, and local governments. Consistent with PDD-63, close cooperation and coordination are also essential for a robust and flexible infrastructure protection program.

1.6.3 Overall FEMA Organization

Figure 1-1 depicts the FEMA organization existing prior to the recent Presidential transition and new Administration. With new FEMA leadership assuming control, the FEMA organization will be subject to change. Considering the above, each of the Directorates is further divided into Divisions and Branches, which are discussed in more detail in the business function section (Section 1.12.2) of this *FEMA IT Architecture* document.

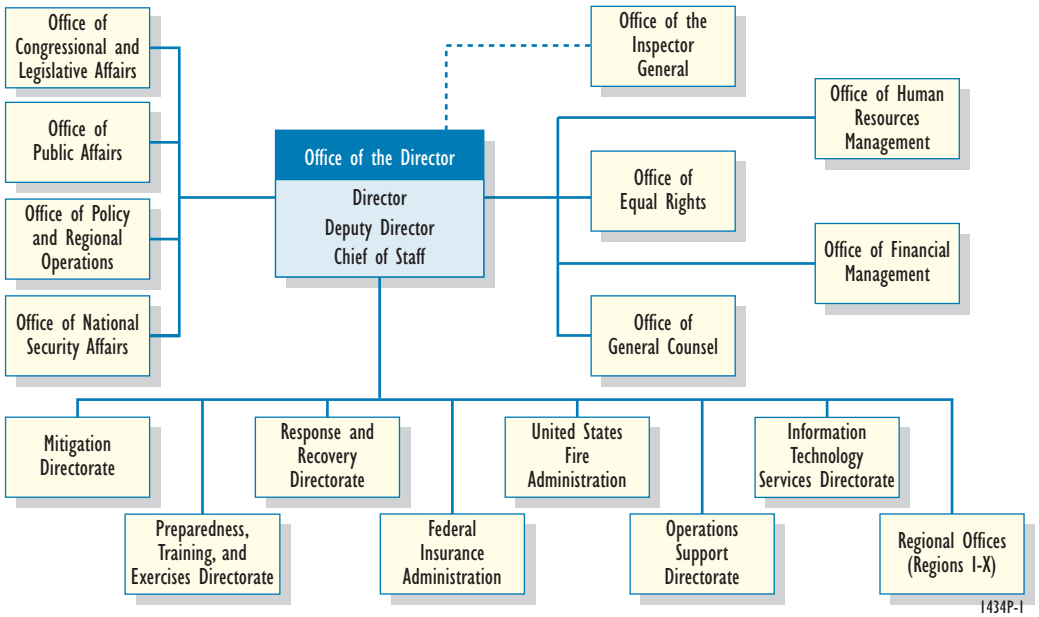


Figure 1-1. FEMA Organization at the Director, Directorate, Region, and Administration Levels

1.6.4 Missions and Responsibilities of Individual FEMA Organizational Entities

Table 1-1 identifies the major missions of the Directorates and Administrations identified in Figure 1-1. At the Directorate and Administration levels, FEMA organizational entities have a requirement for large and diverse information flows, both within FEMA and with external FEMA enterprise partners. Additionally, the information flow must generally be timely, accurate, and precise. Also, the information exchange is often executed under emergency operational circumstances (see Section 1.6.6).

Table 1-1. Missions for FEMA Directorates and Administrations

Directorate or Administration	Mission Statement
Office of the Director	Provide leadership and direction to reduce the loss of life and property from all types of hazards through a comprehensive, risk-based, all-hazards emergency management program of mitigation, preparedness, response, and recovery.
Congressional and Legislative Affairs	Coordinate FEMA's ongoing emergency management dialogue with the U.S. Congress, and coordinate implementation of FEMA's legislative program.
Public Affairs	Disseminate response and recovery information to the public and news media during and after natural disasters and other emergencies, inform and educate the public about emergency preparedness, and inform the public and constituent groups about FEMA's activities.
Policy and Regional Operations	Support the Director and Agency managers by conducting agency-wide planning; developing policy; implementing strategic initiatives; ensuring Regional coordination; and building partnerships with and among State and local governments, non-government organizations, business, and industry.
National Security Affairs	Serve as the focal point for FEMA activities related to Continuity of Government (COG), Continuity of Operations (COOP), and contingency programs by ensuring that these activities are (1) coordinated within the Agency and with appropriate Executive Branch organizations and (2) are uniform and consistent with national security policy and FEMA positions on all-hazards initiatives.
Inspector General	Serve as an independent and objective audit, investigative, and inspection unit relating to FEMA programs and operations for the purpose of promoting economy, effectiveness, and efficiency, or preventing and detecting fraud, waste, and abuse in FEMA programs and operations.
Human Resources Management	Plan and direct human resources programs to maintain a workforce capable of performing the Agency's assigned mission while advancing the Agency's commitment to its employees and the public.
Equal Rights	Serve the Agency and the nation by promoting affirmative employment, a discrimination-free workplace, and equal access to FEMA programs and benefits.
Financial Management	Promote sound financial management and accountability throughout the Agency by providing financial and acquisition-related guidance, information, and services to FEMA management and the Agency's customers.
General Counsel	As a staff element of FEMA, render legal advice and assistance on all matters related to Agency programs and operation.
Mitigation Directorate	Develop, coordinate, support, and implement policies, plans, and programs to eliminate or reduce the long-term risk to human life and property from natural and technological hazards, and support the Director in making mitigation the cornerstone of emergency management.

Table 1-1. Missions for FEMA Directorates and Administrations (Continued)

Directorate or Administration	Mission Statement
Preparedness, Training, and Exercises Directorate	Provide the leadership, policy, financial and technical assistance, training, readiness, and exercise support to strengthen (1) community and Tribal readiness through preparedness and (2) the professional infrastructure of trained and tested emergency workers, community leaders, and public citizens who can prepare for disasters, mitigate against disasters, respond to a community's needs after a disaster, and launch an effective recovery effort. Develop and implement customer service initiatives.
Response and Recovery Directorate	Develop and maintain an integrated operational capability to respond to and recover from the consequences of a disaster, regardless of its cause, in partnership with other Federal agencies, State and local governments, volunteer organizations, and the private sector. Maintain the deployable systems needed to support response activities such as the Mobile Emergency Response Support (MERS) Detachments. Manage the Urban Search and Rescue Task Force Program.
Federal Insurance Administration	Manage a Federal program to provide consumer-oriented flood insurance in participating communities.
United States Fire Administration	Provide leadership, coordination, and support for the nation's fire prevention, control, and emergency medical services (EMS) activities.
Operations Support Directorate	Provide logistics, security, health and safety, and other mission support services essential to the accomplishment of the Agency's all-hazards emergency management program.
Information Technology Services Directorate	Provide agency-wide support for IT services and systems for routine operations and in all-hazards emergency and disaster situations. Provide leadership and direction for management of IT resources, automated data processing (ADP), telecommunications and information services, and systems necessary to support and accomplish FEMA's mission.
Regional Offices	Accomplish, within the Region, the national program objectives established for the Agency by the Director. Establish an all-hazards approach to emergency management throughout the Region through close working relationships with other Federal agencies, State and local governments, private industry, and local volunteer organizations in the implementation of FEMA policies and programs.

1.6.5 FEMA IT Management Team

The ITS Directorate is designated as the primary development authority and management authority for the *FEMA IT Architecture*. Lead responsibility is assigned to the ITS Management Division with the cooperation and assistance of the Program Management Group, the Operations Division, and the Engineering Division.

Under FEMA Instruction 1610.13, the ITS Directorate is tasked to provide technical, planning, and policy presentation support to the Information Resources Board (IRB).

FEMA Instruction 1610.13 defines the authority of the chairperson and designates the membership and responsibilities of the FEMA IRB. The FEMA CIO serves as the chairperson. The primary objectives of the IRB are to:

- Assist the CIO in the performance of FEMA's responsibilities under the ITMRA, the revised OMB Circular A-130 dated November 28, 2000, the *Paperwork Reduction Act,* and the *Government Paperwork Elimination Act.*
- Provide senior-level oversight of FEMA's IT to promote the improvement of the Agency's practices in modernization, use, sharing, and performance measures
- Oversee development of the *FEMA Strategic Plan* that links IT and associated funding
- Strengthen the management of information resources to ensure accountability
- Promote the management of information and IT as strategic investments to pool resources, share experiences, and exchange ideas
- Identify opportunities for cross-cutting cooperation in using IT to support common functions and to integrate IT on an agency-wide corporate basis.

The IRB provides advice to the Chairperson. The Chairperson makes the consensus and view of the Board known to the Director and takes them into account in carrying out the CIO's responsibilities under ITMRA, the *Paperwork Reduction Act,* and the *Government Paperwork Elimination Act.* IRB membership includes:

- Principals:
  - — Chairperson, Chief Information Officer
  - — Deputy Associate Directors, Deputy Administrators, and Office Directors for:
    - Mitigation Directorate
    - Response and Recovery Directorate
    - Preparedness, Training, and Exercises Directorate
    - Operations Support Directorate
    - Information Technology Services Directorate
    - Federal Insurance Administration
    - United States Fire Administration
    - Office of Policy and Regional Operations
    - Office of National Security Affairs
    - Office of Financial Management
    - Office of General Counsel
    - Office of Emergency Information and Public Affairs (delegate)
    - Office of Human Resources Management (delegate)
    - Office of Inspector General (delegate)

- Alternate:
  - — Senior staff member (Division level or above) as designated by the head of the organization.

The IRB-sponsored Information Systems Policy Advisory Group (ISPAG) is responsible for:

- Developing and presenting recommendations
- Providing technical advice
- Identifying information resources issues that should be presented to the full Board
- Meeting with other information systems groups to enhance the subject matter knowledge of the IRB.

1.6.6 FEMA Operational Environment for IT Systems

With FEMA's mission to respond to disasters and emergencies that may be of national scope and significance and that may potentially threaten Continuity of Government (COG), FEMA IT systems and telecommunications resources must be designed, implemented, and integrated in due consideration of a full spectrum of contingencies that may arise. This is a critical architectural factor for development and implementation of *FEMA IT Architecture* and network systems. The IT systems architects and engineers must know and understand the critical operational environmental factors and circumstances under which the system must operate.

This section briefly identifies the operational environmental factors that must be considered in the development of IT systems. It should be understood that not every FEMA business function is deemed as mission critical, nor does every FEMA business function require a robust and redundant IT support capability. On a day-to-day basis, most of FEMA's business functions are well handled in a normal business office environment. However, the potential always exists that FEMA will need to respond to contingencies that are extraordinarily severe. These contingencies place the most stringent of demands on mission-critical IT systems.

Major IT architectural implications for the following representative set of operational environmental factors are provided in Appendix J:

- Adverse weather conditions
- Local, State, and/or Regional infrastructure potentially destroyed or inoperable with a need to operate in a transportable environment
- Need for operations in a remote or rural environment (perhaps requiring a Disaster Field Office [DFO])
- Need for operations in a large destroyed urban environment (e.g., earthquake) other than at FEMA Headquarters or a Regional Office
- Virtual/synthetic environment (for training, exercises, and simulations)
- Contingency operations and alternate facilities
- Office environment (e.g., FEMA Headquarters and Regional Offices including National Flood Insurance Program [NFIP] Regional Offices and Emmitsburg).

Many of the operational environmental factors often occur in combination. For example, adverse weather conditions such as a large hurricane can render infrastructure for an entire region inoperable and necessitate establishment of mobile and transportable support facilities.

1.7 FEMA IT ARCHITECTURAL GOALS AND OBJECTIVES

This section briefly identifies the major goals and objectives underlying the development of the *FEMA IT Architecture*. Consistent with the requirements of the ITMRA and OMB guidance, this *FEMA IT Architecture* documents the fundamental relationships among FEMA's business and management processes and IT. The major goals and objectives identified also establish the foundation for the Agency's evolution to e-FEMA.

The major goals and objectives of the *FEMA IT Architecture* are to ensure:

- Alignment of the requirements for FEMA's information systems with the processes that support FEMA's missions
- Adequate interoperability, redundancy, and security of FEMA's information systems (consistent with the requirements for information assurance and CIP)
- Application and maintenance of a collection of standards (including technical standards) by which FEMA will evaluate and acquire new systems and re-engineer existing systems.

1.8 FEMA IT ARCHITECTURAL PRINCIPLES

This section and Appendix H of the *FEMA IT Architecture* establish the basic architectural principles upon which future FEMA IT systems will be designed, built, and acquired and upon which legacy IT systems will be re-engineered. The architectural principles identified in Appendix H provide a stable foundation upon which FEMA developers, engineers, and integrators can make important IT systems design and implementation decisions. These principles are expected to evolve as FEMA's mission and business functions evolve. They will be periodically reviewed, and their designation as FEMA IT architectural principles will be the responsibility of the CIO as advised by the FEMA IRB.

The FEMA CIO and IRB anticipate that an open systems, disciplined, and standards-based IT architecture will best meet FEMA's needs for designing and developing future information systems, for re-engineering legacy systems, and for achieving future integration and interoperability among systems across the broad and distributed FEMA enterprise. The open systems approach to IT systems across the FEMA enterprise is a fundamental architectural principle that must be employed. It follows that a closed-system, proprietary approach is strongly proscribed unless all reasonable avenues of opportunity for development of an open systems approach have been systematically eliminated and the approach has been agreed upon by the CIO in consultation with the IRB. Waivers and exceptions to the requirement to be open will be granted only under the most extraordinary of circumstances. Cost/benefit factors and operational exigencies may enter into this decision.

The architectural principles defined in Appendix H are mandatory for compliance. Except as indicated, the principles apply to new systems and any new development, interface, or integration

of legacy systems. If a legacy system does not require re-hosting or new development, then these principles do not apply.

1.9 SNAPSHOT OF INITIAL TO CURRENT *FEMA IT ARCHITECTURE*

In assessing and describing the status of the initial FEMA IT and Network Technology Architecture (NTA), it is important to appreciate that the information and network architecture met mission-critical operational requirements. Progress has been made since the development of the initial *FEMA IT Architecture*, and there is considerable ongoing effort to streamline and integrate systems. Figure 1-2 provides a snapshot or view of the initial architecture.

From Figure 1-2, the following major characteristics of the architecture may be inferred:

- Since the development of the initial *FEMA IT Architecture*, *Version 1.0*, FEMA is expending considerable effort to develop and integrate a number of enterprise-wide systems and activities including:
  - National Emergency Management Information System (NEMIS), which is operational in its Version 2 release
  - The Integrated Financial Management Information System (IFMIS)
  - The Logistics Information Management System (LIMS)
  - The Facilities Management (discontinuing term FACMAN) System
  - The FEMA Geographic Information System (GIS) with support from the Map Service Center (MSC) and the Map Analysis Center (MAC). An integrated capability is needed.
  - Office of Human Resources Management (OHRM) corporate data bases supported by various information systems and servers. Development is being initiated to convert this to the Personnel Resources Information Systems Mart (PRISM).

  More details on these systems are provided in Appendix M.

- Enterprise-wide systems were not as well integrated as desired. This largely reflects their current state of development. The ITS Directorate intends that the enterprise systems be better integrated in the target architecture environment.

- The FEMA Network Architecture consists of separate sub-networks, including the FEMA Switched Network (FSN) and the FEMA Router Network/Multiplexer Network. Satellite communication and high frequency (HF) radio are also supported. Together, the networks are being enhanced to increase operational requirements for voice, video (e.g., tele-conferencing), and data. The network can be configured to provide limited Quality of Service (QoS) through manual reconfiguration of switches and multiplexers.

- FEMA had a basic problem resolution process and infrastructure to support FEMA networks, including a help desk and use of Remedy to assist in tracking problems.

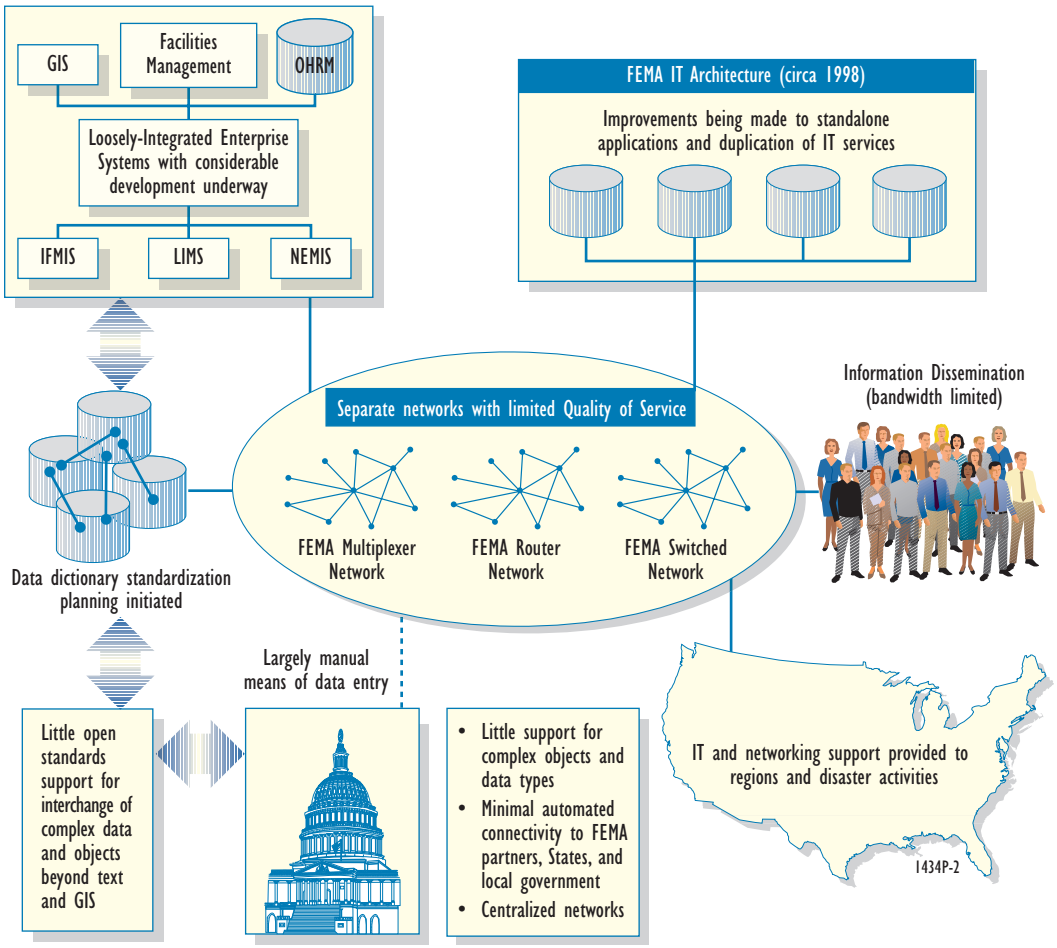


Figure 1-2. Snapshot of Initial to Current FEMA IT Architecture

- FEMA had the capability to establish standalone communications in a disaster area where the communications infrastructure might be destroyed or out of order.

- Although improvements are in progress, the current FEMA Network Architecture is bandwidth-limited should the following IT applications be implemented:
  - — Multimedia applications and graphics-intense interchange
  - — Public information dissemination of multimedia objects such as streaming audio and video
  - — Data-intense GIS applications (e.g., interactive GIS)
  - — Intelligent distributed collaboration and visualization applications
  - — Integrated voice, video, and data applications
  - — Digital library applications where an enterprise-wide document management or text search capability might be incorporated
  - — Virtual reality (VR) applications such as three-dimensional (3-D) simulations for fire-fighting or tele-presence.

- The current FEMA network architecture is largely centralized in its national operations and maintenance (O&M). To date, security concerns have mostly limited establishment of Extranets, Virtual Private Networks (VPNs), and gateways to FEMA enterprise partners and State/local governments (with coordination of the Regional Offices). However, recent decisions were made by the ITS Directorate to initiate planning for VPNs. Partly as a result, much of the data from external sources that are received in paper format must be manually scanned and/or re-keyed. The data that is received electronically from FEMA partners is mostly received as e-mail with attachments (most as word-processed documents).

- Configuration management of systems and networks is being enhanced to provide for a more standardized enterprise-wide solution.

- Although progress is being made, data dictionaries for enterprise-wide systems and especially for standalone systems are not as well standardized and harmonized as desired.

- Numerous standalone systems (e.g., program-centric systems) in the various FEMA organizations have a need for common IT architectural components such as digital signature, document management, correspondence and action tracking, configuration management, and text search but appear to be duplicating efforts in a non-standard fashion. With the implementation of FEMA's GPEA Plan and e-government efforts, improvements are anticipated in this area.

- There was little support for open systems standardized approaches to automated interchange of complex mixed-mode documents and data sets beyond text and some GIS interchanges. Text is largely interchanged through word processor formats and not open systems approaches such as Standard Generalized Markup Language (SGML) and more recently Extensible Markup Language (XML). XML is an application of SGML intended to replace Hypertext Markup Language (HTML) on the Web.

- Considering recent progress, there is less reliance on declaring tools, even if proprietary, to be the FEMA IT enterprise standard, as opposed to defining standard approaches to document and data interchange.

- Electronic records, documents, and data in FEMA IT systems and databases are not locked through secure digital signatures, date-time stamping, and secure hash mechanisms. FEMA understands that this is a common problem for many other Federal agencies, and data protection and integrity issues are widely recognized to be a concern for the CIP Program. In addition, implementation of the Agency's GPEA Plan and other e-government initiatives may help remedy these problems.

1.10 FEMA TARGET IT ARCHITECTURE AND REQUIREMENTS FOR ENHANCED AUTOMATION

This section of the *FEMA IT Architecture* provides the target vision and requirements for enhanced automation. This target vision was validated since the publication of the initial *FEMA IT Architecture, Version 1.0*. FEMA and its enterprise partners share a common set of goals and objectives with regard to emergency planning and operations, including the four major phases of CEM, i.e., Mitigation, Preparedness, Response, and Recovery. In an enterprise-sense, FEMA wishes to exploit IT consistent with the evolving National and Global Information Infrastructure (NII/GII) and ongoing efforts to develop digital government as articulated by the December 1999 Presidential Directive on e-government. These principles are fully congruent with the ITMRA and the revised OMB Circular A-130 dated November 28, 2000, which requires that Federal agencies produce IT architectures to guide their resource allocation decisions.

FEMA, in cooperation with its enterprise partners, intends to develop and implement capabilities for secure and intelligent, bi-directional, electronic document and data interchange in a widely-distributed collaborative environment. Consistent with the requirements of GPEA, other public law, and national-level directives, the model for creating, managing, and using such electronic documents and data must work in a legal and regulatory framework.

The new Administration has signaled that e-government is a top priority for the Administration. FEMA, through this *FEMA IT Architecture*, will provide the leadership to fully realize e-government and e-FEMA.

As shown in Figure 1-3, FEMA and its enterprise partners share common problems associated with distributed collaboration on, and interchange and representation of, complex information (including text, graphics, and multimedia objects as well as engineering, GIS, mathematical, radiological, human services, medical, chemical and environmental, weather, geologic, and transportation data) in an intelligent and searchable electronic format. This concept is the essence of *creating documents and data sets once in their most intelligent form, effectively managing them throughout their life cycle, and deriving maximum downstream re-use of the information.*

FEMA has vital concerns about how electronic objects can stand up to data integrity and security management requirements in an electronic environment that is widely distributed in a telecommunications sense and exploits video tele-conferencing (VTC) and other high bandwidth collaborative technology. It is reasonable to believe that FEMA's enterprise partners share these concerns. With recent court cases, FEMA is also aware that it is no longer adequate to assume that printed copies of the records will be legally acceptable in a court of law instead of the electronic records. Accordingly, the *FEMA IT Architecture* adopts a strong standards-based approach, the requirements for an integrated data repository and warehouse, and secure portal connectivity with FEMA's enterprise partners, in future development and implementation. Widely implemented, internationally-accepted, open systems standards for the representation, interchange, collaboration, and visualization of documents and data in an intelligent electronic format are recognized as a challenge at all levels of government and throughout industry.

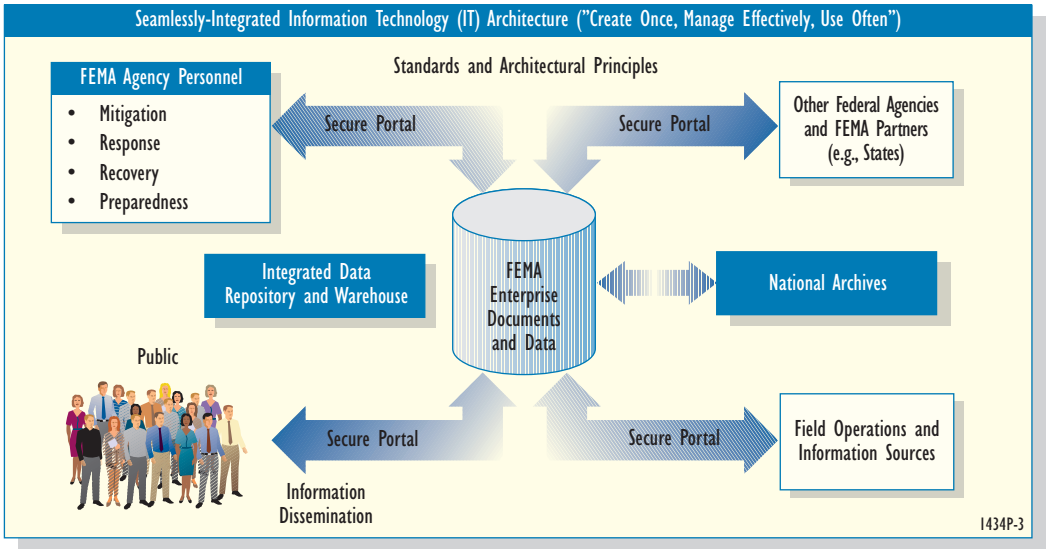


Figure 1-3. FEMA Enterprise Architectural Concept of Creating, Managing, and Using Documents and Data in an Intelligent Format

Integration of IT Systems and Processes into the Network Architecture

As illustrated in Figure 1-4, for FEMA integration of IT to create data once in its most intelligent form, manage it across its life cycle, and then gain maximum re-use (mitigation activities being an excellent example), IT systems demand a robust, distributed networking and communications environment. Within FEMA, IT systems must be seamlessly integrated with the network environment. Section 3 of this *FEMA IT Architecture* identifies the target network architecture in more detail. Figure 1-4 further identifies some of the anticipated benefits in achieving this level of integration.

Target Architecture Vision

Figure 1-5 depicts an overall architectural vision for FEMA that seamlessly integrates IT systems, data, and architectural components in a robust networking and communications environment. The fundamental goal of the target architecture is to support the notion of *Comprehensive Emergency Management* in the areas of mitigation, preparedness, response, and recovery as articulated in the *FEMA Strategic Plan*. In reference to Figure 1-5, the target *FEMA IT Architecture* has the following major characteristics:

- **Well-Integrated Enterprise-Wide Systems and Services.** Currently, there is considerable ongoing effort to develop and integrate a number of distributed enterprise-wide IT systems. In the target architecture, FEMA enterprise-wide systems will be well-integrated and interoperable to the extent required by the design requirements as approved by the CIO in consultation with the IRB. This means that the systems support the concept of "*Create Once, Manage Effectively, and Use Often"* in a seamless and secure manner. In the target architecture, all FEMA enterprise systems are considered mission-critical and must meet the stated operational environmental factors for the functions that they support. They shall be designed, developed, tested, and integrated in accordance with the *FEMA IT Architecture*. They shall also be developed, maintained, and operated to afford CIP and assurance consistent with EO 13010 and PDD-63. In the system development and integration process, it is anticipated that FEMA enterprise

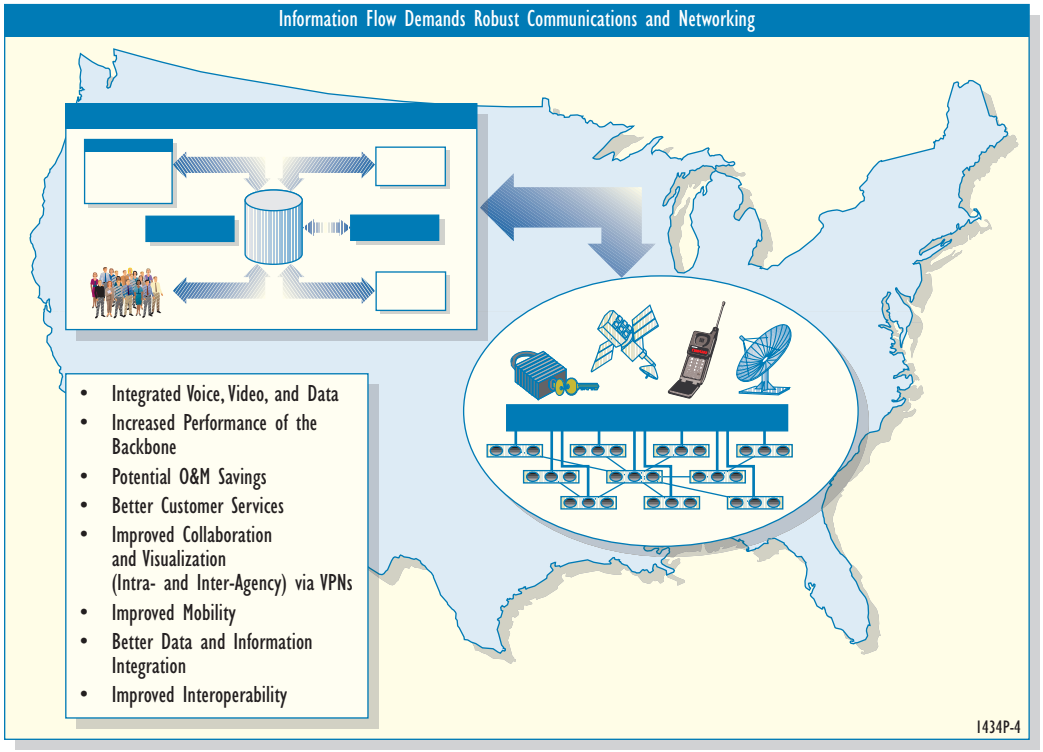


Figure 1-4. Integration of IT Systems Environment into the Networking Environment

systems will assume the lead role in developing standardized services and capabilities (i.e., common re-usable architectural components) that will be made broadly available to other clients such as standalone program-centric systems and users across the enterprise. In this regard, FEMA recognizes that its investment in the NEMIS infrastructure and environment presents significant opportunities for FEMA to integrate other currently isolated and standalone areas of FEMA information systems. The NEMIS infrastructure serves as a major application within the Agency's evolution into e-FEMA. In the development of the *FEMA IT Architecture*, the NEMIS project is a significant development and integration project for defining and implementing a *FEMA IT Architecture* baseline and e-FEMA. In implementation of the *FEMA IT Architecture*, the ITS Directorate is open to innovation and good ideas from other organizational elements and enterprise systems.

As shown in Figure 1-5, FEMA enterprise-wide IT systems include:

— National Emergency Management Information System (NEMIS), which is operational in its Version 2 release. The FEMA ITS Directorate will continue a series of Joint Application Development (JAD) sessions across FEMA in an initial effort to baseline future NEMIS requirements and releases. Depending on funding, potential candidates for future enterprise-wide functionality to be incorporated in future NEMIS releases include:
  - Automated Grants Management (disaster and non-disaster) and Acquisition Management
  - Virtual Private Networks (VPNs) with States and other Federal agencies

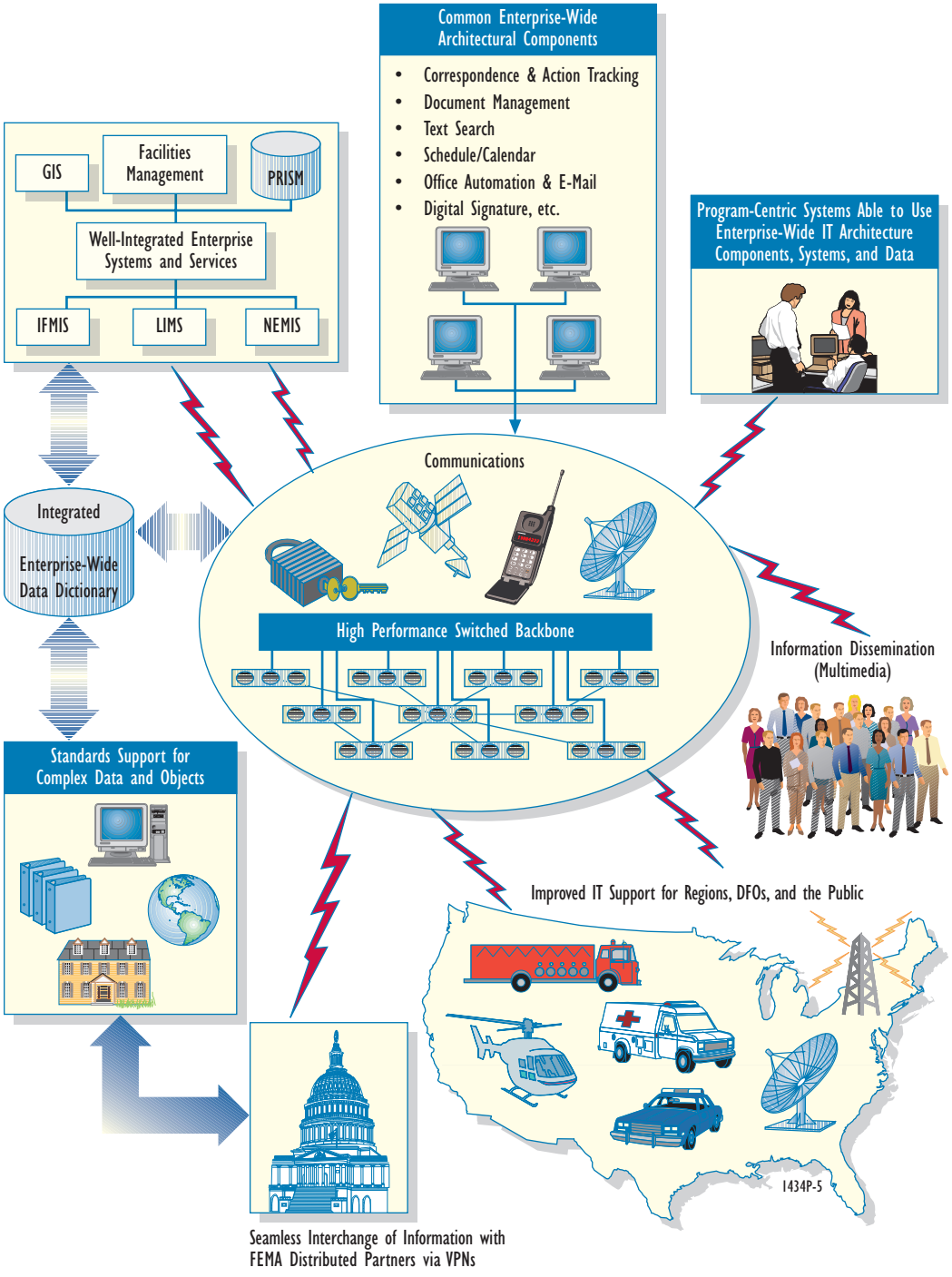


Figure 1-5. FEMA IT Architecture Target Vision

  - An Exercise and Training Module integrated with response and recovery functionality to simulate emergencies in a virtual environment and to support distributed exercise planning, operations, reconstruction, and analysis
  - Improved interfaces and/or some reallocation of functionality with other enterprise systems (e.g., LIMS, IFMIS, Facilities Management System, GIS, and PRISM)
  - Improved enterprise-wide functionality in such areas as digital libraries, security and information assurance, data warehousing, workflow management, text search, document management, digital signatures, and correspondence and action tracking.
- The Integrated Financial Management Information System (IFMIS)
- The Logistics Information Management System (LIMS)
- The Facilities Management System
- The FEMA Geographic Information System (GIS), with support from the Map Service Center (MSC) and the Map Analysis Center (MAC). The current GIS capability is somewhat fragmented across FEMA. An enterprise-wide, integrated capability is needed. FEMA formally began the process of planning its integrated Enterprise GIS capability when the CIO formed the agency-wide GIS Working Group in the fall of 1999. The working group is currently providing oversight of an enterprise GIS requirements analysis followed by a strategic plan and implementation plan. This process, when completed in 2001, will provide direction for the implementation of the FEMA Enterprise GIS in accord with the *FEMA IT Architecture* requirements and guidelines. In addition, this project is also proposed as one of FEMA's Target Architecture Capabilities.
- Office of Human Resources Management's corporate resource data base supported by various information systems and servers. This is also proposed as one of FEMA's Target Architecture Capabilities, and will be called the Personnel Resources Information Systems Mart (PRISM).

Improved Communications and Networking. In the target architecture, communications and networking will be supported by an integrated high-performance switched backbone where work is currently underway. Progress has been made in this area since the publication of the initial *FEMA IT Architecture, Version 1.0*. Section 3 of this *FEMA IT Architecture* describes the target network architecture in more detail. Depending on funding, the target network architecture is planned to support integrated voice, video, and data applications and higher bandwidth applications, including streaming multimedia to the public for information dissemination purposes as well as distributed interactive simulations (DISs) for exercises. Core capabilities are planned to be provided through the implementation of Asynchronous Transfer Mode (ATM) technology. In the target architecture, increased emphasis may be placed on Personal Communications System (PCS) technology and Global Positioning System (GPS) for operations in the field. Increased emphasis will also be placed on CIP aspects of the FEMA network architecture.

Consideration for Legacy Telecommunications Systems as New Capability Is Added. Important legacy telecommunications systems such as HF radio and the National Warning System (NAWAS) will be preserved for the time being to meet continuing critical operational requirements. The goal is to have a network environment that meets all of the operational requirements, operates better, and costs less across the spectrum of emergencies. In the target architecture, benefits can be expected at all operational levels as illustrated in Figure 1-6.

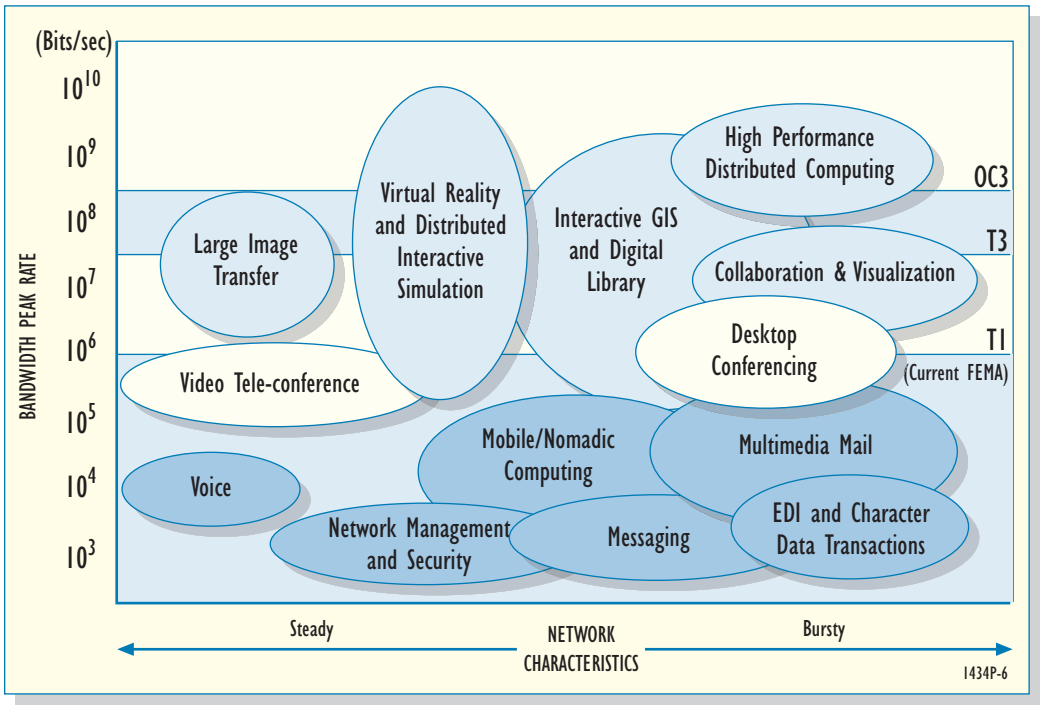


Figure 1-6. Bandwidth Requirements and Network Characteristics for Various Advanced Information Technologies

- **Bandwidth Less of a Concern for Advanced IT Applications.** In the future network architecture, bandwidth limitation will be less of a factor and the network will be designed to provide adaptive QoS. This approach and philosophy are consistent with the Next Generation Internet (NGI) and Internet2 projects. Depending on funding, the proposed target network architecture will be scalable and will support bandwidth-intensive and potentially demanding IT applications such as:
  - — Multimedia applications and graphics-intense interchange
  - —Public information dissemination of multimedia objects such as streaming audio and video
  - — Data-intense GIS applications
  - — Intelligent distributed collaboration and visualization applications
  - — Integrated voice, video, and data applications
  - — Future digital library applications where an enterprise-wide document management or text search capability might be incorporated
  - — DISs for exercise support
  - — Future VR applications such as 3-D simulations for fire-fighting or tele-presence purposes.

  Figure 1-6 depicts the relative requirements for bandwidth for various IT architectural components that have been identified. The figure also depicts the relative requirements for the transmission of data across the network to be *steady* as opposed to *bursty* in nature.

- **Potential for Increased Connectivity.** As noted above, the current FEMA network architecture is largely centralized in its national O&M. With security concerns such as firewalls

properly considered, and policies and procedures properly implemented, the target network architecture provides opportunities to potentially establish Extranets, gateways, and VPNs. Opportunities should be explored with the Regions to establish connectivity with FEMA's enterprise partners and with State/local governments. This should result in improved performance and information interchanges in an automated fashion.

- **Responsiveness to Consensus on Standards.** FEMA hopes that the target *FEMA IT Architecture*, with its Technical Reference Model (TRM), will help to bring consensus among the Agency's business partners on standards to support the interchange of electronic documents, data, and complex objects in a seamless and more intelligent fashion. The goal will be to employ the concept of *"Create Once, Manage Effectively, and Use Often"* and to minimize the need for scanning and re-keying of data. FEMA will be attentive to a consensus that emerges. Within its limited resources, FEMA, including its Regions, may engage with its business partners in prototyping and piloting components of the new IT and NT architectures.

- **Engineering Concerns Addressed.** In the target architecture, a number of ancillary issues lingering from the current architecture will be addressed and resolved. These include:
  - Configuration management of systems, networks, data, and metadata shall be consistently performed and shall employ a standardized enterprise-wide approach.
  - Data dictionaries for enterprise-wide systems and standalone, program-centric systems shall be standardized and harmonized to achieve semantic and syntactic data integrity across the enterprise.
  - In development of IT systems, there will be increased emphasis on employing standardized life-cycle models. This might include increased emphasis on employing processes and procedures from the Software Engineering Institute (SEI).
  - A number of standalone or program-centric information systems and data bases are expected to be consolidated and/or retired. Standalone systems and program-centric systems will continue to be permitted, though they will be mandated to employ common enterprise-wide architectural components if they need such services. Common architectural services are identified below.
  - Consistent with the architectural principles stated in Appendix H, there will be increased and improved support for open systems standardized approaches to automated interchange of complex mixed-mode documents, objects, and data sets beyond current free-form unstructured text and GIS data.
  - Substantially increased emphasis will be placed on IT systems security engineering to meet the goals and objectives of the Critical Infrastructure Protection (CIP) Program.

- **Tools and Open Systems Standards.** Due to its inability to affect the design of IT products, FEMA will continue its general practice of declaring tools to be FEMA IT enterprise standards. Where it appears practical to do so, FEMA will specify open system standards.

- **Improved Data Integrity Over the Life Cycle.** Consistent with the direction of the CIP Program, electronic records, documents, and data in FEMA IT systems and data bases will have increased levels of ensured data integrity. With adequate policies and procedures in place, the architecture will evolve to support secure digital signatures, date-time stamping, long-term

archival access, and secure hash mechanisms. FEMA will respond promptly to initiatives of other Federal agencies to help address this common problem.

Identification of Common Architectural Components

In preparing the initial *FEMA IT Architecture*, *Version 1.0,* the ITS Directorate conducted a series of interviews with senior managers, analysts, and engineers across the organization, including the Regions. The respondents identified a common set of IT needs that can be met through an approach of standardization across the enterprise. In general, the respondents embraced the concept of a common enterprise approach to addressing common IT needs, as opposed to *going it alone*. The list below presents the IT architectural needs that were expressed most often. This list was validated for the updated *FEMA IT Architecture, Version 2.0*. In addition, several of the needs depicted below have been identified as new specific projects and are included in FEMA's Target Architecture Capabilities. Detailed discussions of the Target Architecture Capabilities are included in Volume 2, Appendix P. The architectural needs are:

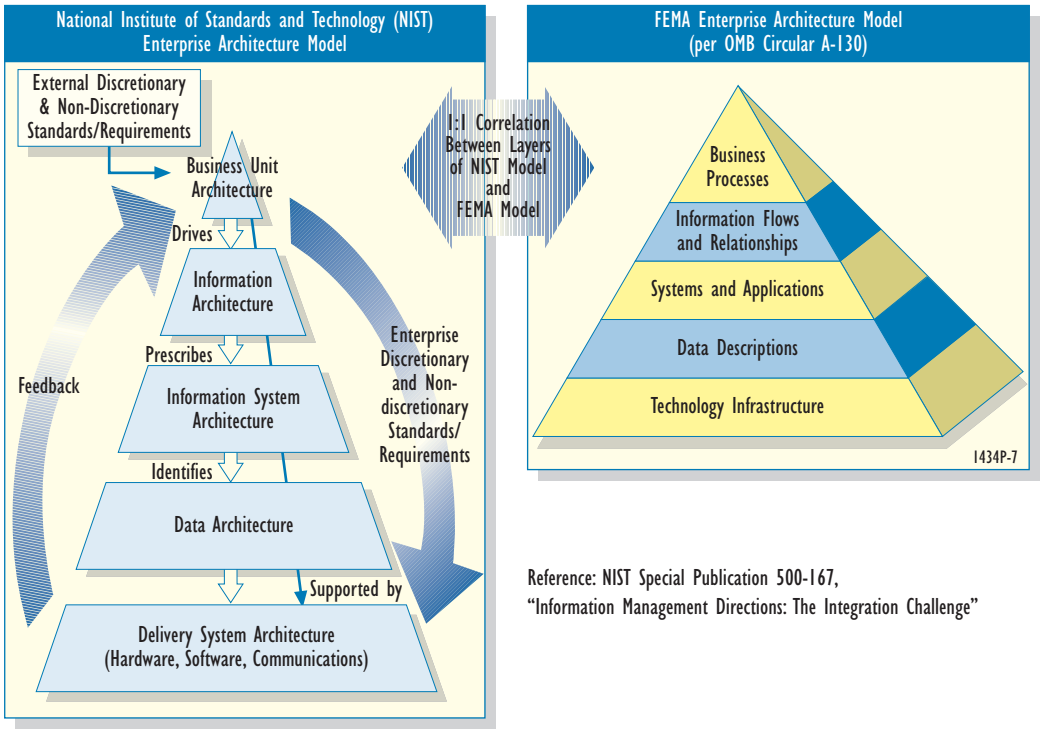
1. Digital library services for creating, managing, and using complex mixed-mode documents and data sets including enterprise-wide search and retrieval services and data warehousing
2. Enterprise-wide data dictionary standardization
3. Correspondence and action tracking services
4. Grant management system services
5. Increased access to, and integration of, GIS products and services
6. Better office automation products
7. Improved ability for collaboration and visualization of documents and data sets (especially GIS data sets) in a distributed environment
8. Improved support for distance learning activities
9. Access to an enterprise-wide Document Management System (DMS)
10. Support for digital notaries and digital signature services
11. Improved electronic capture and support of legacy documents and paper
12. Improved utilization of the Internet for high-volume information dissemination and for collaborative and planning activities
13. Improved support for secure electronic commerce and electronic data interchange (EDI)
14. Enterprise support for multimedia integration, including streaming audio and video
15. Improved document and data support for mobile users
16. More direct connectivity to FEMA's business partners and the States through Extranets and VPNs
17. Adoption of standardized tools in such areas as configuration management and systems engineering
18. Advanced Call Center/Integrated Voice Response.

1.11 MAPPING OF FEMA TARGET IT ARCHITECTURE TO THE NIST MODEL

As illustrated in Figure 1-7, the *FEMA IT Architecture* model is patterned after and correlates well to the National Institute of Standards and Technology (NIST) Enterprise Architecture, which is documented in NIST Special Publication 500-167, entitled *Information Management Directions: The Integration Challenge*.

As indicated in OMB guidance, the NIST model has been widely promoted in the Federal government as a management tool to illustrate the interconnectivity of the business, information, systems, data, and NT environments of an enterprise and their relationships. The NIST model provides a five-tiered framework for building an integrated set of information and IT architectures. As illustrated, the five tiers are defined separately but are interrelated and tightly interwoven. The common threads between the layers are discretionary and non-discretionary standards (e.g., the TRM and standards profiles).

As illustrated in Figure 1-7, the *FEMA IT Architecture* model also has five tiers. Each of these five tiers is similar to the NIST model, but they have been tailored to be consistent with the terminology defined in OMB guidance. As with the NIST model, IT standards are the threads that bind the tiers of the *FEMA IT Architecture*.



Reference: NIST Special Publication 500-167,
"Information Management Directions: The Integration Challenge"

Figure 1-7. Mapping of Target FEMA IT Architecture to the NIST Model

1.12 MAJOR IT ARCHITECTURAL COMPONENTS

1.12.1 Methodology

This section of the *FEMA IT Architecture* addresses the five major architectural tiers as required by the OMB guidance (see Figure 1-7). To facilitate the development, maintenance, and implementation of the *FEMA IT Architecture*, FEMA initiated development of a *FEMA IT Architecture* Data Base as illustrated in Figure 1-8.

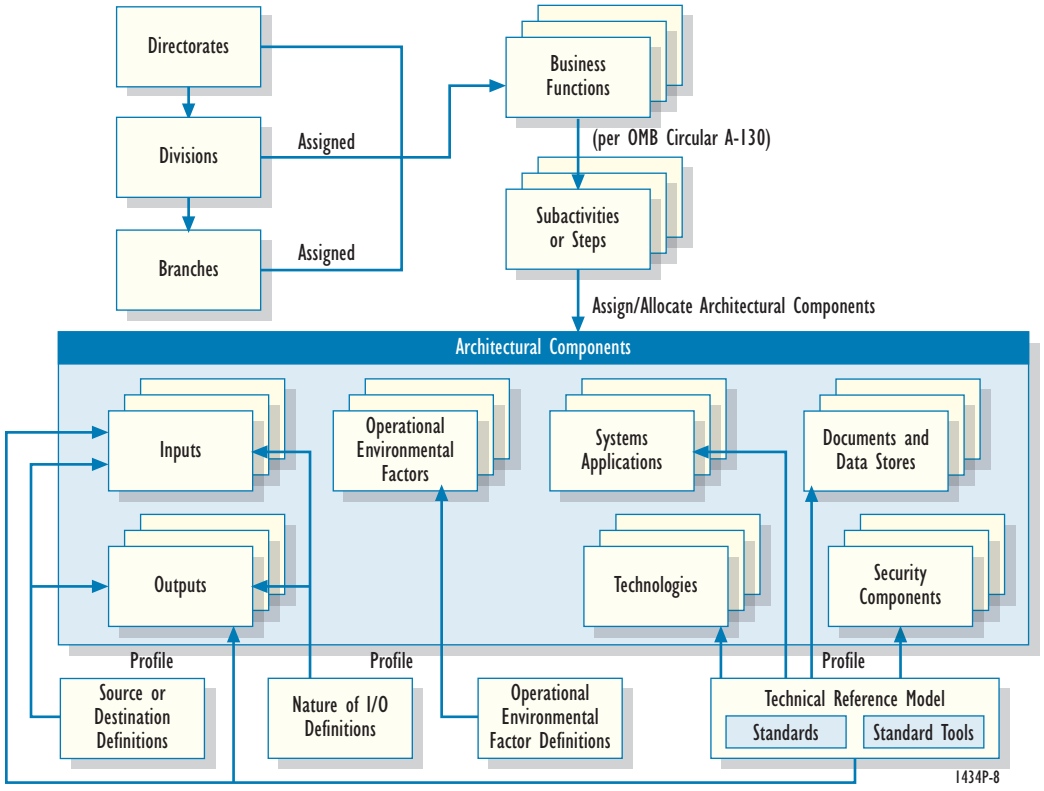


Figure 1-8. Structure of FEMA IT Architecture Data Base

The *FEMA IT Architecture* Data Base depicted in Figure 1-8 provides an automated road map to help address the architectural tiers.

The *FEMA IT Architecture* Data Base provides a framework to help define and allocate re-usable IT architectural components to business functions and subactivities. As illustrated in Figure 1-9, it also helped serve as a template for conducting a series of structured discussions on the current and target *FEMA IT Architecture*. Structured discussions were conducted with nearly all of

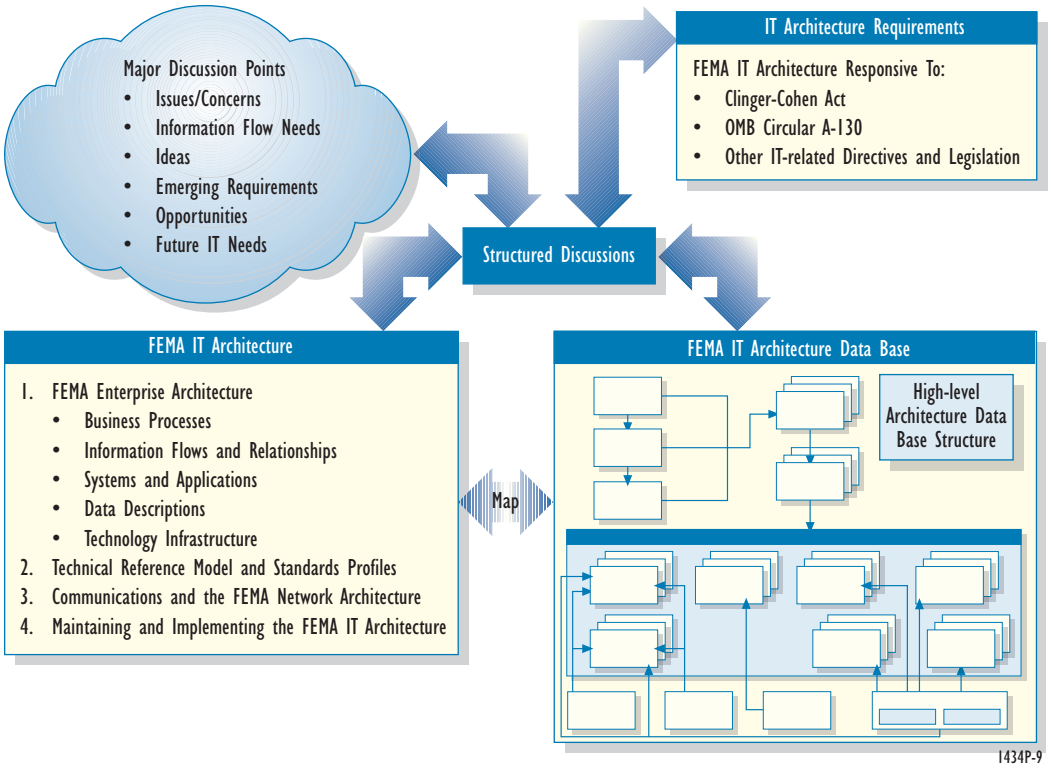


Figure 1-9. Framework for Conducting Structured Discussions with FEMA Organizational Elements

FEMA's organizational elements, including the Regional Offices. The updated *FEMA IT Architecture, Version 2.0,* validated the information obtained from the structured discussions.

Structured discussions were conducted on the following architectural components:

- **Business Functions** (e.g., What are the high-level business functions and how are they allocated or assigned to FEMA organizational elements?)

- **Subactivities** (e.g., What are the important subactivities for the business functions?)

- **Inputs and Outputs** (e.g., What are the required internal FEMA and external business partner inputs for a business function or subactivity? What outputs are produced? Who receives and uses the outputs? This discussion addressed the *information flow* architectural level described in OMB guidance.)

- **Operational Environmental Factors** (e.g., Which factors apply to the business function or activity? See Appendix J for candidate listing of operational environmental factors.)

- **Systems and Applications** (e.g., Which existing and planned systems and applications apply to, or support, the business function or subactivity and how do they apply?)

- **Documents and Data Stores** (e.g., Which document(s) or data store(s) apply to, or are maintained by, the business function or subactivity? What is the nature of the document or data store? What is the source of information in the document or data store?)

- **Technologies and Security Components** (e.g., Which technologies and security architecture components apply to the business function or subactivity? Which are currently being applied and which are of future interest as potential standardized architectural components?)

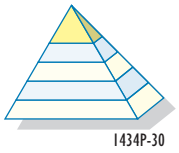
The structured interview process was coordinated through the FEMA Information Resources Board (IRB) to gain increased *buy-in* across FEMA for the final results of the effort. With regard to FEMA's business processes, the goal of this structured interview effort was to:

- Gain an increased and thorough understanding of FEMA's business functions at the senior staff level
- Identify vital information flow requirements needed to support business functions
- Identify senior staff concerns about current and emerging information systems and networks
- Identify new opportunities for streamlining and simplifying the IT systems development process
- Identify needs and requirements for future automation activities
- Identify opportunities for technology insertion
- Identify opportunities for development and standardization of enterprise-wide architectural components that address cross-cutting business needs (such as planning, collaboration, visualization, data capture, interfacing with business partners, reporting, auditing, search and retrieval, etc.).

In updating the *FEMA IT Architecture, Version 2.0,* and in developing FEMA's Target Architecture Capabilities, a similar interview process as described above was also used.

1.12.2 FEMA Business Processes

1.12.2.1 Introduction


1434P-30

This section of the *FEMA IT Architecture* addresses FEMA's core business processes and functions. As noted above, the mission of FEMA is to***: "Reduce the loss of life and property and protect our institutions from all hazards by leading and supporting the Nation in a comprehensive, risk-based emergency management program of mitigation, preparedness, response, and recovery."*** FEMA's core business revolves around the four major business processes contained in the FEMA mission statement: ***mitigation***, ***preparedness***, ***response***, and ***recovery***.

While FEMA is a small agency, its information and communications requirements are large and operationally demanding. Development of the *FEMA IT Architecture* considered:

1. **The large number of subordinate staff business processes and procedures needed to address the four major business functions.** FEMA currently has allocated over 500 business functions to staff elements at the Directorate/Administration, Division, and Branch levels in support of the four high-level business functions. The *FEMA Missions and Functions Manual* provides a comprehensive listing of the assigned missions and business functions

down to the FEMA Branch and Section level. A number of these functions will be addressed and analyzed at a high level below.

2. **The large number of FEMA external business partners and Federal, State, and local governments that FEMA must interchange information with not only under crisis management circumstances but also during normal day-to-day operations.** The scope of the FEMA enterprise is large, and IT systems and networks are mission-critical resources. It is conservatively estimated that FEMA interchanges information with well over 200 external organizations ranging from voluntary organizations like the American Red Cross to the National Weather Service. Through FEMA's 10 Regional Offices, FEMA interchanges large volumes of information with State and local governments such as geospatial data (e.g., floodplain maps) and engineering studies and analyses in providing mitigation support. During crises, the Regional Offices are an important focal point for providing rapid response and recovery support. This support is information intense as well as often sensitive and time-critical, raising potential issues associated with security and the need to ensure a robust networking and IT systems environment. During a crisis, elected officials, the public as a whole, and the affected population want to know: What is happening? What are the options? How can they help? and When is relief in sight?

3. **The large number and broad scope of documents and data that FEMA either receives or produces for the over 200 external organizations with which FEMA routinely interacts.** Today, much of the information flow is still in paper and some of it must still be physically signed. An appreciable amount of the information is faxed. Increasingly, more and more information is being interchanged in office automation formats and as e-mail, though interoperable standards are sometimes lacking. A large volume of information is also exchanged verbally with increasing trends toward video tele-conferencing (VTC) and Internet-based approaches for collaboration. Today, comparatively little information is interchanged in direct computer-to-computer interpretable and processible format. New tele-registration and data transfer activities under NEMIS are a notable exception. It is widely recognized across the emergency management community that IT standardization is important to achieve increased efficiencies across the enterprise. It is generally less recognized that such standardization will necessitate some business process re-engineering.

   With the implementation of GPEA, FEMA developed its GPEA Implementation Plan for providing the electronic option, which includes electronic signature, for information collections and other information dissemination. FEMA must be GPEA compliant by October 2003. FEMA's GPEA Plan is discussed in more detail in the Executive Summary of this volume.

4. **The difficulty in achieving standardization and consensus across the FEMA enterprise on IT and networking solutions.** While everyone wants to achieve improved information flow and interoperability, organizational dynamics and comparatively small IT architectural differences across the enterprise frequently frustrate this effort. For example, minor differences in the compression algorithm for various commercial off the shelf (COTS) e-mail packages may mean that file attachments cannot be reliably interchanged and opened across the enterprise much less digitally signed and protected. In addition, FEMA must be leery of

fragile software that simply does not operate as advertised or is laced with *bugs*. This *FEMA IT Architecture* addresses this problem area by establishing FEMA as being proactive to help achieve consensus on IT and network standards across the enterprise. In fact, FEMA is a major sponsor of the Emergency Information Infrastructure Partnership, which focuses on a dialogue on technology and information needs of the entire emergency management community and may be a significant contributor to this effort.

1.12.2.2 Analysis of FEMA Core Business Processes and Functions

This section provides a high-level analysis of FEMA's core business processes and functions. The reader is referred to the *FEMA Missions and Functions Manual* for a detailed listing of the missions and business functions assigned down to the Branch and Section levels. The following are the general conclusions and observations about the core business functions. In particular, the IT-significant features and aspects of the core business functions are addressed.

Mitigation

The *National Mitigation Strategy* is the guiding document in making mitigation become the cornerstone of emergency management at FEMA. An analysis of the *National Mitigation Strategy*, discussions with Mitigation Directorate and Regional Office personnel, and an analysis of the mitigation-related business functions indicate that IT and communications are vital components of this core business function. Major IT-significant features and aspects of mitigation include the following:

- **Mitigation combines the science of discovery of all hazards, their analysis and risk assessment, with sound engineering practices to develop and implement mitigating measures.** Mitigation is an information intense activity covering all major engineering disciplines and strives to represent knowledge and information. Digital library science with robust and intelligent search and retrieval is a central technology that is needed. Also important are computer-aided engineering models, graphics tools, economic forecasting tools, data mining and trend identification tools, multimedia display formats, text search and retrieval tools, DMSs, and interactive Geographical Information System (GIS) products.

- **Mitigation activities require close collaboration, coordination, and liaison across a broad spectrum of activities at the Federal, State, and local government levels.** In the current environment, much of this collaboration is direct face-to-face through attendance in meetings. In an electronic environment, this requirement places a premium on distributed intelligent collaboration and visualization tools; IT standards to interchange scientific, technical, and engineering information; distributed planning and reporting tools, integrated voice, video, and data applications; and interoperability and connectivity of IT systems and networks (such as Extranets and Virtual Private Networks [VPNs]).

- **Within FEMA, mitigation heavily relies on an enterprise GIS to capture, store, and retrieve information on hazards.** The use of GIS places a premium on data capture of very large amounts of geographically-oriented information from all sources including National Technical Means, ensuring data quality, organizing data appropriately on a map, pinpointing the data on the map with an acceptable level of precision and accuracy (necessitating

technologies such as Global Positioning System [GPS] and interferometric techniques), storing it, analyzing it, discovering trends, making it interactively available in the field, interchanging it with FEMA business partners, and using it in such programs as the National Flood Insurance Program (NFIP) and fire-fighting programs.

- **The Mitigation Directorate is responsible for the establishment, in conjunction with FEMA's Regional Offices, of a nationwide, map-based Hazard Identification and Risk Assessment Program which forms the foundation for FEMA's *National Mitigation Strategy*.** This program supports Federal, State, and local emergency management interests through the provision of useful products and information. The GIS initiative to support mitigation is expected to place a significant stress on FEMA's IT systems and supporting network infrastructure in the near future. The growth curve for use of GIS products and services is definitely up. The demand for accurate, interactive, and detailed products is very high not only in other Directorates within FEMA, but also with external customers. Mitigation Directorate personnel indicated that significant aspects of their GIS initiative which impact FEMA's IT systems and networking infrastructure include:
  - A **current focus is on map modernization** to speed up the flood mapping process, lower the cost, and increase the accuracy of results.
  - A further emphasis is on **providing more support to local areas**; thus high-bandwidth, interactive GIS product information dissemination will become increasingly more important in the future. Map Service Center (MSC) activities will be extended to the provision of Flood Insurance Rate Maps as digital raster products over the Internet.
  - The Mitigation Directorate has the requirement to **establish a national inventory of structures and related data sets** needed to support the *National Mitigation Strategy*, the NFIP, Response and Recovery Operations, and a credible national risk assessment and loss program. This is clearly a data intensive effort.
  - There is a **heightened need to use existing and emerging remote sensing assets** to the fullest. The sensing assets that are being considered tend to produce massive amounts of data which must be interchanged and handled within FEMA's IT and network environment (Internet and Intranet), as well as be disseminated in an interactive manner.
  - In that the **information element of elevation is so critical** in many flood mitigation planning and preparation scenarios, the collection, processing, and use of this data element is of high priority. The FEMA Mitigation Directorate has decided to employ and fuse data from Interferometric Synthetic Aperture Radar (IFSAR) and Light Detection and Ranging (LIDAR) collection systems. This is still an experimental effort. The goal is to achieve a 15 centimeter vertical accuracy on a 1 meter posting. The volume of data expected to be received and processed as part of this collection program is massive.
  - A future objective to which IFSAR and LIDAR are likely to contribute is the configuration of a **single pass, multiple-use collection capability** which can both assist with mitigation and rapid damage assessment (e.g., situation assessment) to support response and recovery. This will place a need for more interactive, near real time access to the data by FEMA teams and partners working in the field.
  - The Mitigation Directorate plans **to evaluate fused IFSAR and LIDAR data to gain additional GIS information** such as terrain elevation, structures characteristics, soil permeability and water retention, ground cover categorization, flow diversion, and other infrastructure conditions. When combined with other collection programs, the initial data

volume collected is estimated to be on the order of petabytes (e.g., 1,000 terabytes). While initial data volume may be on the order of petabytes, after processing, vectorization, and compression, the data volume is likely to be less than 10 terabytes. This will likely stress existing IT systems, storage and archiving capability, collaboration and visualization, and networking, particularly if the GIS information is accessed and retrieved in a dynamic and interactive manner (as is envisioned). Additional analysis of the impact of this volume of data on the FEMA network is required.

- **With regard to mitigation, FEMA must manage and coordinate activities covering a number of public laws, directives, and programs** including the Flood Mitigation Grant Program under the *National Flood Insurance Reform Act*, EO 11988 (Floodplain Management), EO 12699 (Seismic Safety of New Federal Buildings), National Earthquake Hazards Reduction Program, the Dam Safety Program, and others. In general, the scope of the mitigation business function with regard to the list of programs calls for **a comprehensive and well integrated, enterprise-wide, IT solution for Grants Management** that will be a part of NEMIS, Version 2, and incorporates:
  - Authoring standards for developing and packaging the grant application which may contain scientific and technical material covering all hazards and disciplines
  - Signature by the originating authority
  - Submission to FEMA (ideally via electronic means)
  - Receipting and date-time stamping of the grant application
  - Workflow within FEMA to process the application
  - Review and collaboration of the grant application (distributed review and collaboration)
  - Tracking, monitoring, and reporting in consonance with new *Government Performance and Results Act (GPRA)* results
  - Engineering and scientific analysis of the results
  - Digital library storage and retrieval of documents and data sets (including multimedia objects which may be attached) associated with the grant program
  - Application of security architecture measures to maintain document and data integrity confidentiality (where required), audit trails, legal and regulatory records, etc., associated with the program or grant
  - Broad information dissemination to get the results out to partners at the State and local level
  - Training associated with the results
  - Financial operations and payment
  - Project closeout.

In updating the *FEMA IT Architecture, Version 2.0,* and developing FEMA's Target Architecture Capabilities, Automated Grants Management, to include both disaster and non-disaster, was identified as a high priority program for FY 2002. As the program is developed, the various possible grant's components identified above will be further evaluated and analyzed for possible inclusion in the new system.

- **Mitigation must be fully integrated with response and recovery and preparedness activities.** In particular, the Mitigation Directorate identified an emerging need to collect verification and validation information for a disaster. From an IT architecture perspective, this places a premium on the concept of creating information once in its most intelligent form,

managing it effectively across its life cycle, and then gaining maximum re-use. With this approach, not only should mitigation activities support response and recovery, Research and Recovery (R&R) Directorate operations should provide verification and validation data to guide future mitigation activity. Interoperable and stable document and data standards are necessary to achieve this synergy. The Mitigation Directorate is responsible for development and integration of the Mitigation Response into the *Federal Response Plan*.

- **The Mitigation Directorate reported that it is actively supporting the Response and Recovery Directorate in developing Emergency Information Requirements for various disasters.** Hurricane information reporting requirements have been developed in draft form and are under evaluation and review. This effort is currently looking at 10 different hazards, 15 different time periods, and 67 different information categories. This effort is also developing accuracy requirements for the reported information. Formats for data interchange are also under consideration and development. From an IT perspective, IT systems within FEMA will need to capture, maintain, and process this information, some of which is expected to be large in volume.

- **Mitigation also advises national model building code organizations, national planning groups, and engineering and scientific communities and industry**, on program policy involving mitigation standards and techniques. The Mitigation Directorate coordinates the development and advancement of technical (construction-related) standards and guidance with Federal and State agencies, international activities, State building code authorities, construction organizations, and various testing groups. The Mitigation Directorate has similar requirements for interchange of scientific, technical, graphical, mathematical, and engineering information covering all hazards including chemical, biological, radiological, and all natural disasters. One of the major goals and objectives of the FEMA Technical Reference Model (TRM) is to promote open systems standards and consensus on preferred approaches to interchange this type of technical and engineering information.

- **Training, workshops, and seminars are an important component of mitigation business functions and activities**, thereby establishing a potential need for distance learning, multimedia presentations, and distributed collaboration and visualization technologies covering integrated voice, video, and data applications. It is hoped that such technologies will afford cost/benefits in the future. These technologies will need to be fully integrated with preparedness, training, and exercise support.

Preparedness, Training, and Exercises (PT&E) Support

Discussions with PT&E Directorate and Regional personnel and an analysis of PT&E-related business functions indicate that IT and communications are also vital components of this core business function. Major IT-significant features and aspects of preparedness, training, and exercise support include the following:

- **PT&E provides the leadership, policy, financial and technical assistance, training, readiness, and exercise support to strengthen (1) community and Tribal readiness through preparedness and (2) the professional infrastructure of trained and tested emergency workers, community leaders, and public citizens who can prepare for disasters,**

mitigate against disasters, respond to a community's needs after a disaster, and launch an effective recovery effort. As is the case with mitigation, PT&E is an information intense activity, with the added dimension to incorporate robust and timely communications to support planning, control, and operations of exercises and various training events. A great deal of interaction with State and local governments is necessary to assist in planning and preparing for emergencies. This role is expected to expand as technology provides better means of communication and interaction over distance. Closer working relationships are necessary in the areas of planning and guidance procedures and documentation. Today, this is a largely manual process. Central to the business processes of PT&E in a future electronic environment are distance learning technologies; distributed modeling and simulation approaches; interactive GIS systems; multimedia approaches; video streaming (live and on-demand); DMS; the Internet for information dissemination; Internet technologies as a tool for distributed planning, collaboration, and visualization; tele-presence and VR technologies; and digital library science with robust and intelligent search and retrieval.

- **PT&E activities require close collaboration, coordination, and liaison across a broad spectrum of activities** including the Regions; Federal, State, and local government; voluntary organizations; and FEMA's business partners. In the structured interviews, PT&E Directorate personnel reported that their Directorate routinely communicates with more external agencies and activities than any other FEMA organization. FEMA Regional personnel validated the need for exchange of large amounts of information with the States and local governments as part of infrastructure planning, guidance documents, and exercise planning and operations. Accordingly, PT&E's requirement for real time and near real time collaboration to support exercises and training events is firmly established. This requirement places a premium on distributed intelligent collaboration and visualization tools; IT standards to interchange exercise and training information; distributed exercise planning, reconstruction, and reporting tools; integrated voice, video, and data applications; and interoperability and connectivity of IT systems and networks (such as Extranets and VPNs). The PT&E Directorate and the Regions are advocates for establishment of Extranets and VPNs. They clearly recognize that security and firewall issues need to be addressed (i.e., as a part of the Critical Infrastructure Protection [CIP] Program). One example PT&E suggested was development of a distance learning server at the National Emergency Training Center (NETC) in cooperation with the U.S. Fire Administration (USFA) to serve training and higher education activities for the Training Division and National Fire Academy.

- **In structured discussions, PT&E personnel emphasized the need for interactive flow of ideas and strategies and the need to conduct planning with FEMA's partners/customers.** Such dialogue is essential to success in developing enterprise-wide document and data interchange standards.

- **The PT&E Directorate reported establishment of a new business function capability entitled Capability Assessment for Readiness (CAR).** The intent of this initiative is to develop a core capability for States to assess themselves in 13 major areas. The project will have a data base component, and a potential issue is portability to local government. With the *Government Performance and Results Act*, PT&E personnel indicated that performance-based reporting measures are increasingly being levied on the States. Consistent with the direction of

the FEMA TRM, additional emphasis needs to be placed on defining and achieving consensus on the standards for the required structure and content of the reports.

- **With regard to preparedness, training, and exercise support, FEMA must manage and coordinate activities covering a number of public laws, directives, and programs.** These include the Community Assistance Program, Radiological Emergency Preparedness Program (REP), Chemical Stockpile Emergency Preparedness Program (CSEPP), EO 12657 (with regard to liaison with the Nuclear Regulatory Commission), post-Cold War programs and projects involving Department of Defense (DOD) activities, the Performance Partnership Agreement/Cooperative Agreement Process, Comprehensive Environmental, Response, Compensation, and Liability Act (CERCLA) hazardous materials preparedness program, the Emergency Management Institute (EMI) (e.g., PT&E manages EMI), Emergency Management Training (EMT) portion of FEMA's Performance Partnership Agreements, MERS training program, community Corrective Action Program, the Legislative Authorities Program (in coordination with the *Defense Production Act*), the Industrial Capacity Assessment Program, and others. In general, the scope of the PT&E and Regional Office business functions with regard to the list of programs calls for a comprehensive and well integrated IT solution for preparedness, training, and exercise support.

- **PT&E develops and manages programs that provide funding assistance through FEMA's Office of Financial Management (OFM) to State and local governments** for the design, development, acquisition, operation, and maintenance of emergency management facilities, telecommunications systems and capabilities, participation in exercises, and other emergency equipment capabilities. As with the Mitigation Directorate, the PT&E Directorate and the Regional Offices can benefit from a well-integrated, enterprise-wide Automated Grants Management System, which is planned for NEMIS, Version 2, and now included in FEMA's Target Architecture Capabilities.

- **The PT&E Directorate in close coordination with the Regional Offices has the requirement to improve the ability of Federal departments and agencies, State and local governments, volunteer organizations, and the private sector to respond to emergencies through a comprehensive all-hazards, multi-scenario exercise program.** This includes:
  - — Developing exercise packages and scenarios for use by State and local governments
  - — Developing, maintaining, and distributing an integrated multi-year exercise calendar
  - — Developing procedures for capturing and recording data on the exercises
  - — Providing on-scene exercise controllers and observers
  - — Providing, or arranging for, financial, logistics, and communications support during the exercise
  - — Performing reconstruction and analysis of the exercise and generating after action reports
  - — Disseminating the results
  - — Developing and managing a Corrective Actions Program and a reporting system.

For real world exercises, the basic IT requirements are to capture the data, maintain it, and provide digital library services for re-use. There is also a vital need to protect and preserve such exercise information. Of potential interest to the PT&E Directorate and the Regional Offices is

evaluation of distributed interactive simulation (DIS) technology developed by (and currently used by) DOD which provides a set of protocols enabling an automated and interactive approach to conducting exercises. DIS can integrate data bases such as GIS data bases and provide a virtual or synthetic environment in which all exercise participants can interact in a realistic manner. The costs and benefits of this sort of approach need to be carefully assessed.

- **In structured interviews, PT&E Directorate personnel indicated that they provide facilities management services at Mt. Weather.** Major subactivities include financial management; administrative support; facility operations and maintenance; warehousing, procurement, and supply management; property management; facility management; and customer care services (e.g., fire protection, medical services, billeting, food service, etc.). The PT&E Directorate is an important user of the Facilities Management System. From an IT perspective, the following were suggested as potential automation initiatives:
  - Increased use of digital document libraries and archives to reduce the amount of paper copies
  - Better integration of Time and Attendance Reporting with the Facilities Management System
  - Tighter integration of LIMS and IFMIS with the Facilities Management System
  - Desired ability to archive all facility drawings (estimated at about 10,000 drawings) and make them accessible for environmental and safety purposes on the Intranet.
  - Increased use of Electronic Data Interchange (EDI) technology for acquisitions with support for digital signatures on electronic documents, drawings, and purchase orders.

- **In structured interviews, PT&E Directorate personnel indicated that they were frequent users of VTC capability.** With their mission areas of distributed training, preparedness, and exercise planning and operations, they are also strong proponents for development of integrated voice, video, and data applications, particularly as the FEMA GIS data base is enhanced. They cautioned that bandwidth on existing networks is a concern for high quality VTC and will become more of a concern as large data objects are interactively searched, retrieved, and visualized.

- **Training, workshops, and seminars are a vital component of preparedness.** The Training Division within the PT&E Directorate has the mission to provide national leadership in the development and delivery of training necessary to ensure that individuals and groups with key emergency management responsibilities acquire the requisite skills. This is a large mission area, and the reader is encouraged to look at the full scope of subordinate business functions for this Division in the *FEMA Missions and Functions Manual.* The scope of the functions and responsibilities justifies the Training Division's interest in advanced IT technologies in areas such as distance learning; multimedia presentations; distributed collaboration and visualization technologies; integrated voice, video, and data applications; training data bases; digital libraries; electronic methods for registration at conferences; and the use of the Internet.

Response and Recovery (R&R)

The *Federal Response Plan* is the guiding document defining FEMA's core business functions for response and recovery. Discussions with R&R Directorate, ITS Directorate, and Regional personnel and an analysis of R&R-related business functions in the *FEMA Missions and Functions Manual* indicate that IT and communications are vital components of these core business functions. Please refer to the *FEMA Missions and Functions Manual* for a detailed set of business functions.

Figure 1-10 depicts the major activities defined in the *Federal Response Plan*. Also shown are the 12 Emergency Support Functions (ESFs) and the application of Recovery and Mitigation Programs as part of the response cycle. Response and recovery requires the efforts of State and Federal agencies; private, public, and non-profit organizations; and individuals. Following a Presidential disaster declaration, 28 Federal agencies (led by FEMA) support State and local organizations through one or more of the ESFs. Private and voluntary organizations provide appreciated goods and services to disaster victims.

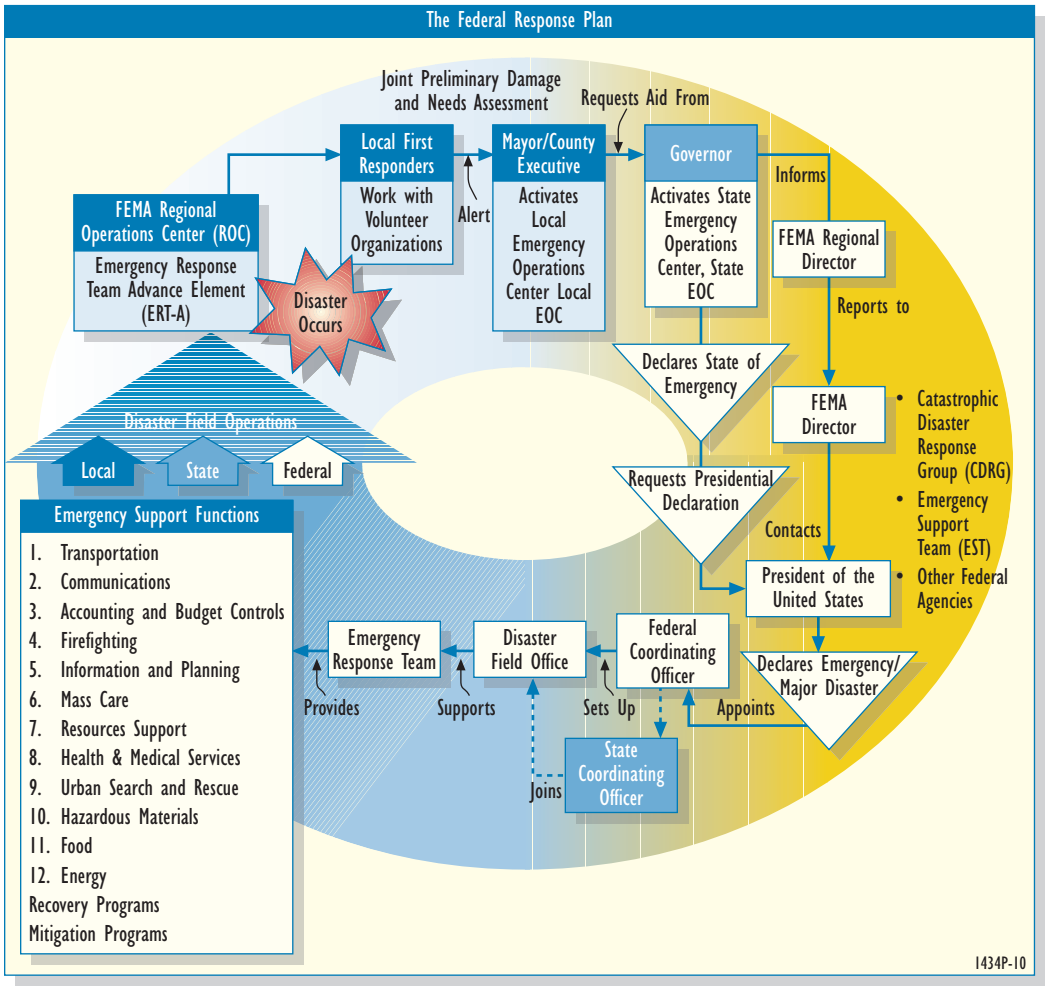


Figure 1-10. Federal Response Plan Activities

Under the *Federal Response Plan*, R&R efforts are coordinated by FEMA's Regional and Headquarters staff and managed by a Presidentially-appointed Federal Coordinating Officer (FCO). This activity implies a large information flow, which must be supported in a timely and responsive manner by IT systems and networks. The combined *response* efforts ensure the rapid provision of safe water, food, shelter, and essentials to disaster victims, and assist in the restora-

tion of basic community services from sewage treatment to accessible roads. The *recovery* effort aids the long-range restoration of eligible facilities including public roads, bridges, and hospitals. Such efforts support the restoration of economic and community stability.

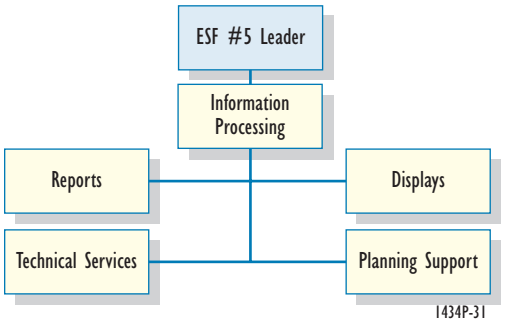
The R&R Directorate strongly supports recommendations to integrate voice and data networks, to establish VPNs with FEMA's business partners, and to move to the ATM protocol. In the structured interviews, R&R indicated that these initiatives will improve the way that FEMA works with other *Federal Response Plan* agencies and responds to disasters.

Major IT-significant features and aspects of FEMA's response and recovery core business functions include the following:

Response Activities

- **Timely communications and networking are critical to the process for response and recovery during time of a disaster.** In Figure 1-10, essential elements of information (EEIs) must flow from box to box. The need for adequate, timely, robust, and reliable communications simply cannot be understated and is a major driving factor in the development of this *FEMA IT Architecture*. Connectivity and essential communications must be provisioned, maintained, and ensured through the entire chain of command. Requirements for CIP are a vital component of FEMA response activity.

- **Resources are provided by 28 Federal departments and agencies and the American Red Cross.** Essential resources are grouped into 12 ESFs, each headed by a Primary Agency with other agencies providing support as necessary. Federal disaster recovery programs and mitigation assistance are also implemented and integrated under the *Federal Response Plan*. The *Federal Response Plan* is linked to emergency plans of departments and agencies. Each of the ESFs has important information flow and underlying data base support requirements and features. For example, ESF #9 *Urban Search and Rescue* reflects the need for FEMA to have ready access to lists of available Search and Rescue (SAR) assets, with their readiness and logistics considerations. Other ESFs cover important aspects of support for human services (e.g., mass care, health and medical services, food) and infrastructure support (e.g., transportation, public works and engineering, communications, etc.). From an IT perspective, FEMA works closely with its business partners on defining EEIs for each of the ESFs, the required structure and content of the messages, methods of communication for the data elements, and formats for information exchange.



- **Particular attention is drawn to ESF #5 *Information and Planning*, which is assigned to FEMA. ESF #5 has major implications for design and development of IT systems at FEMA.** The purpose of ESF #5 is to collect, process, and disseminate information about a potential or actual disaster or emergency to facilitate the Federal government's response and assistance to an affected State. The scope of the *Information and Planning* ESF is to coordinate

the overall information and planning activities at Headquarters, in the Regions, and at Field Offices in support of Federal response operations. This activity is information intensive and includes significant and growing support requirements for an integrated, enterprise-wide GIS capability. ESF #5 activities are grouped, as shown in the accompanying figure, among the following major functions underneath the ESF #5 Team Leader:

— **Information Processing** to collect and process essential elements of information from the State, the other ESFs, and other sources; disseminate it for use by response operations; and provide it as input for reports, briefings, displays, and plans.
— **Reports** to consolidate information into reports and other materials to describe and document overall response activities, and to keep Regional and national offices, including heads of departments and agencies, Congress, and the White House, informed of the status of the overall response operations.
— **Displays** to maintain displays of pertinent information and facilitate briefings using maps, charts, and status boards in a Situation Room and through other means, such as computer bulletin boards or electronic mail, as available.
— **Planning Support** to consolidate information to support the action planning process initiated by Emergency Response Team (ERT) leadership in the field and the Emergency Support Team (EST) leadership in Headquarters.
— **Technical Services** to provide advice on disaster areas including aerial reconnaissance, meteorology, structural engineering, seismology, flooding, dam safety, legal and law enforcement issues, national security issues, and other areas requiring specific information to support response efforts.

- **The Assessment and Analysis Branch in the Operations and Planning Division in the R&R Directorate has the mission to develop and maintain an integrated inter-agency situation assessment capability to support response and recovery operations.** In particular, the Assessment and Analysis Branch is responsible for developing and maintaining emergency operating procedures for ESF #5 including the following functions:
  — Information collection and reporting
  — Situation reporting procedures including the production of a national Situation Report (SITREP)
  — Briefing and displays to support emergency operations
  — Use of predictive modeling and GIS support in disaster operations
  — Standard procedures for documenting disaster operations
  — Procedures for development and production of *Action Planning Documents* and *Incident Action Reports.*

The Assessment and Analysis Branch is also responsible for managing the remote sensing program before emergency situations develop and after disaster operations begin. This program includes overhead photography and other sensing, as required. From an IT systems perspective, the Branch has a significant need to create, manage, and use a large volume of material (text and graphics). The Branch can benefit from advanced digital library technology, interactive GIS, and improved and more accurate and timely methods of collecting information in the field (e.g., employment of PCS, laptops, and GPS for field inspectors to pinpoint locations in disaster areas where normal features such as street addresses and other locating features might be destroyed).

- **In general, the Operations and Planning Division within the R&R Directorate has a large and significant requirement for IT systems and telecommunications support. In coordination with PT&E, the Division also supports training exercises, which require a large information flow.** The reader is referred to the *Mission and Functions Document* for a complete listing of business functions for this Division. Nearly all of the assigned business functions are IT systems-significant. Some of the more significant functions for this Division, which need to be supported by IT systems or telecommunications, include:
  - Planning and Coordination Branch:
    - Policy and briefings on the *Federal Response Plan*
    - Operational planning and response to the consequences of terrorism
    - Point of contact with the Office of National Security Affairs (NS) for COOP planning for the R&R Directorate
    - Inter-agency coordination and support of R&R operations.
  - Emergency Services Branch:
    - Operations support (including mission assignments and action tracking)
    - EST and ERT operations support
    - Emergency response documentation
    - NEMIS usage and data support (Note: NEMIS has data models for Emergency Coordination [EC] and Emergency Support [ES] that are used by the R&R Directorate).
- Operations Centers Branch:
  - Operations of the National Emergency Coordination Center (NECC), Emergency Information Coordination Center (EICC), and the National Warning Center
  - Readiness Team support (including emergency alert and notification procedures).
- Assessment and Analysis Branch:
  - Information and planning (for *Federal Response Plan* Annex, EST Handbook Annex, standard operating procedures, etc.)
  - Development of a rapid situation assessment capability
  - Community relations regarding R&R operations
  - Disaster reporting requirements
  - Remote sensing and reconnaissance support (see above).

- **Within the R&R Directorate, the Mobile Operations Division manages the Mobile Emergency Response Support (MERS) Detachments and the Mobile Air Transportable Telecommunications System (MATTS) deployments.** MERS Headquarters has Operations, Telecommunications, Logistics, and Administration responsibilities. Individual MERS Detachments are under a MERS Chief and consist of Operations, Telecommunications, and Logistics Branches. MERS detachments are part of FEMA's all-hazards mission response capability. In the immediate aftermath of a disaster, there may be a critical need for communications, information and decision support, operations support, and life support. Support for the MERS detachments tends to be IT systems and communications intensive. An analysis of the MERS detachment business functions indicates a number of processes that need to be supported by IT systems and networking. These processes include:
  - Operations:
    - Activity planning and coordination
    - Reports generation
    - Planning support to Regions

- ESF #5 support to the Regional Operations Center (ROC) and Emergency Response Team Advance Element (ERT-A)
- Gathering of information on incidents.

— Telecommunications:
- Install, operate, and maintain satellite systems; telephone systems; very high, ultra high, and high frequency (VHF, UHF, and HF) radios; cross band radio relays; line-of-sight radios; Recovery Channel/Analog Video Broadcast uplink system; VTC system; and local and wide area network (LAN and WAN) connections.

— Logistics:
- Operate and maintain power generation system, water system, fuel system, and heating, ventilation, and air conditioning (HVAC) system, and report on MERS readiness
- Maintain MERS vehicles and report on readiness
- Provide for property accountability (through LIMS).

An analysis of the assigned business functions for the Readiness Coordination Division within the R&R Directorate indicates that this Division also has a large and significant requirement for information. In general, assessment of FEMA's readiness to support response and recovery activities requires that data and information from distributed sources be gathered in a timely manner. The data and information must be critically analyzed to determine readiness measures and capabilities. In an IT systems environment, this requirement places a premium on the ability to create, manage, use, and share data in a distributed and secure collaborative fashion, as well as a decision support capability. Some of the more IT significant business functions of the Readiness Coordination Division include:

— Administrative Team:
- R&R budget formulation and execution
- Input R&R fiscal data into IFMIS
- Development of fiscal reports
- Personnel actions and tracking
- Property accountability during R&R operations
- Coordination of Community Disaster Loans and State Share Loans.

— Correspondence Team:
- Handling of all Congressional, White House, and general public correspondence
- Coordination of Office of the Inspector General (OIG) and General Accounting Office (GAO) reports and audits.

— Strategic Planning and Evaluation Team:
- Implementation of GPRA requirement in R&R operations
- Design of R&R evaluation systems (e.g., setting standards, data analysis, data base design, corrective actions)
- Design and administration of surveys (including customer service surveys)
- Design and management of after action reports.

— Federal Disaster Declaration Policy and Processing Team:
- Support the Director in such areas as Declarations, Turndowns, Appeals, Cost-Share Adjustments, and Requests for Program/Policy Clarifications
- Manage the disaster declaration process.

Recovery Activities

- **The Human Services (HS) Division has the mission to ensure that individuals and families that have been affected by disasters have access to FEMA's human services programs in a timely manner** and that the best possible level of service is provided to applicants in the administration of these programs. This business function includes developing partnerships and exchanging information with the States, voluntary organizations, the private sector, and other Federal agencies that are delivering similar assistance. From a FEMA IT perspective, the HS Division is a major user of NEMIS, and the HS information flow requirements supported by NEMIS are large. The HS Division consists of the Program Guidance and Implementation Branch and three National Processing Service Centers (NPSCs) in Texas, Maryland, and Virginia. With NEMIS support, the Program Guidance and Implementation Branch administers a broad spectrum of human services programs including:
  - Individual and family grant programs
  - Disaster housing program
  - Crisis counseling program
  - Stress management program
  - Disaster unemployment assistance
  - Disaster legal services
  - Cora Brown Fund
  - 403 Audit Program
  - Donations Management Program.

  The Program Guidance and Implementation Branch is also responsible for coordinating benefits to ensure that there is no duplication, interpreting applicable laws, developing business rules, and providing regulations and instructions to Field Offices.

- **Within the HS Division, the three NPSCs provide tele-registration services, eligibility determinations, benefits processing, and helpline support.** The NPSCs help victims begin the process of recovering from disasters. The human services support includes answering calls promptly, listening compassionately, recording data carefully, providing accurate information to callers, and ensuring timely and accurate transmission of callers' data to assistance providers. NEMIS is an integral part of this human services support capability. For example, NEMIS provides a set of screens and a user interface. Data capture is accomplished through an interview process with victims. Within NEMIS, automated eligibility determinations are made through application of a comprehensive set of business rules associated with the Individual and Family Grant and Disaster Housing Program. NEMIS has also developed automated and portable methods of inspection in the field including assessments of damage, which feed the benefits determination process. NEMIS also provides a set of rules and data base for *National Flood Insurance Reform Act (NFIRA)* compliance checking, as well as interfaces to the Small Business Administration (SBA) for loans processing.

  Each of the NPSCs also serves as a Center of Excellence. Texas is the Center of Excellence for Call Center Systems and provides policy for the tele-registration process. Maryland serves as the Center of Excellence for applicant claims processing, including systems improvements and automation for benefits processing. Virginia is the Center of Excellence for Customer Services/Innovation and also administers inspection service contracts.

- **Within the R&R Directorate, the Infrastructure Division conducts Public Assistance (PA) activities related to the repair or rehabilitation of qualifying public and certain private non-profit facilities.** With its comprehensive Infrastructure Support (IS) module, NEMIS provides an omnibus approach to manage FEMA's Infrastructure recovery programs. In particular, the reader is referred to the NEMIS *Functional Description* and *System/Subsystem Specification* for details of this comprehensive support capability. Data elements for IS are defined in the NEMIS logical and physical data model, described in more detail in Section 1.12.5. The following are some of the key features of NEMIS IS capability:
  - NEMIS supports inspectors in the field in the automated capture and submission of the Preliminary Damage Assessment (PDA) and associated cost estimates to repair. The NEMIS approach and data model support geographical pinpointing of inspection data at GPS accuracy levels. NEMIS provides a mechanism to enter this data into a GIS, to manage it, and to make it available for downstream re-use across the enterprise.
  - NEMIS provides the comprehensive ability to create, manage, and use Disaster Survey Reports (DSRs). For example, NEMIS includes a digital library ability to associate incoming documents and data with case folders and databases. As the NEMIS project progresses, there will be tighter integration with the FEMA GIS data base.
  - NEMIS affords the applicant and Regional Offices with maximum visibility into infrastructure recovery efforts through remote access to appropriate and applicable data bases. In this regard, NEMIS also supports briefings, distributed collaboration activity, tele-conferencing, and report generation.
  - NEMIS supports routing and distribution of IS recovery files and data to appropriate authorities and action officers.
  - NEMIS has been developed and integrated using automated workflow methodologies to support infrastructure recovery processes including initiation activity, damage assessment, cost estimating, electronic document and data submission, document and data base development and maintenance, review of documents and data sets, allocation and obligation of resources, tracking and reporting of response activities, and closeout processes.

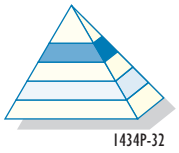
- **The R&R Directorate develops and manages programs that provide funding assistance to State and local governments, as well as to families and individuals.** Some of the recovery activities can be prolonged as exemplified by R&R's establishment of the Northridge Earthquake Long-Term Recovery Area Office as a special project. The R&R Directorate manages a number of disaster-related grant programs under public law. As with the Mitigation Directorate, the PT&E Directorate, and the Regional Offices, the R&R Directorate could benefit from a well-integrated, enterprise-wide Grants Management System.

1.12.2.3 Other FEMA Business Processes and Functions

In addition to mitigation, preparedness, response, and recovery, FEMA organizational elements also perform a number of other business functions that are important to the overall FEMA mission and that are IT and networking significant. Appendix L briefly summarizes the major IT needs and requirements of the other FEMA business processes and functions that were expressed during the structured interviews.

1.12.3 FEMA Information Flows and Relationships

1.12.3.1 Introduction



This section of the *FEMA IT Architecture* briefly analyzes the information used by FEMA in its business processes and the movement of the information internal to and external to FEMA. The relationships among the various flows of information are also described in this section. These information flows indicate where the information is needed and how the information is shared to support FEMA's mission functions.

1.12.3.2 Organizational Entities and Their Information Flows

As highlighted in Section 1.12.2, FEMA Business Processes, information flow is critical to, and a central component of, FEMA's mission and business functions. That section of the *FEMA IT Architecture* briefly discusses high-level information flows associated with mitigation; preparedness, training and exercise support; and response and recovery.

Appendix L identifies high-level information flows associated with other business functions and processes including:

- GPRA reporting
- Insurance operations
- Systems engineering, maintenance, and configuration management of facilities, IT systems, and networks
- Handling of national security information
- Fire prevention and control training
- Training and exercise support
- Financial management
- Interchanges of high-volume GIS map information
- Acquisitions and purchasing
- Grants management.

External Agency Coordination

Across the FEMA enterprise, it is conservatively estimated that FEMA organizational elements interchange information with over 200 other external organizations. In addition, there is a large internal information flow. With this volume of information flow, it is intractable to address all of the relationships among the various flows of information in this document.

For this updated *FEMA IT Architecture, Version 2.0*, it was decided to address the information flow at a high level. Future revisions may address information flow at a progressively more detailed level. Also, FEMA plans to capture the essential information flow elements in its *FEMA IT Architecture* Data Base (see Section 1.12.1 above and the discussion below).

Need to Consider External Partners

With the very large number of external agencies and organizations with which FEMA interchanges information, any discussion of information flow must properly consider external agency concerns. A considerable volume of the information flow requirements and their interrelationships are already well defined in the 12 Emergency Support Functions (ESFs) that are part of the *Federal Response Plan*.

With the guidance and direction of documents such as the *FEMA Strategic Plan*, the *Federal Response Plan*, and the *National Mitigation Strategy*, FEMA is working closely with its business partners to further define the structure and the required information flows. For example, the information flows associated with hurricanes have recently been promulgated for review. This effort is currently looking at 10 different hazards, 15 different time periods, and 67 different information categories. This effort is also developing accuracy requirements for the reported information. As noted above, formats for data interchange are also under consideration and development. In coordination with its business partners, FEMA is also identifying needs and requirements to ensure vital information flow as part of the CIP initiative.

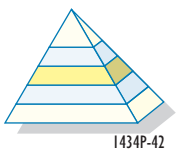
1.12.3.3 Methodology and Information Flow Requirements

As part of the structured interview process, ITS Directorate personnel conducted discussions on the high-level information flow requirements with all of the major FEMA Directorates. The discussions on information focused on identifying the major high-level inputs and outputs for ultimate capture into the *FEMA IT Architecture* Data Base.

Figure 1-11 identifies the scope of the discussions that were conducted on major inputs and outputs. Appendix F summarizes the major high-level information flow requirements for the Directorates and Administrations. Appendix G provides more details on the discussion of documents and data stores (Section 1.12.5) and identifies a large number of documents and data stores that are maintained by FEMA organizational elements. Many of these documents and data stores must be interchanged either internally or externally, also contributing to the requirements for information flow. Lastly, the NEMIS enterprise-wide data modeling approach addressed in Section 1.12.5 also provides a mechanism for identifying and describing the detailed information flow requirements.

1.12.4 FEMA Systems and Applications

1.12.4.1 Introduction



This section of the *FEMA IT Architecture* addresses FEMA enterprise-wide and program-centric applications (and systems). Consistent with the revised OMB Circular A-130, these are applications that capture, manipulate, and manage the business information to support FEMA's mission operations. This section also briefly describes the high-level logical dependencies and relationships among FEMA's business activities, which are supported by the applications and systems.

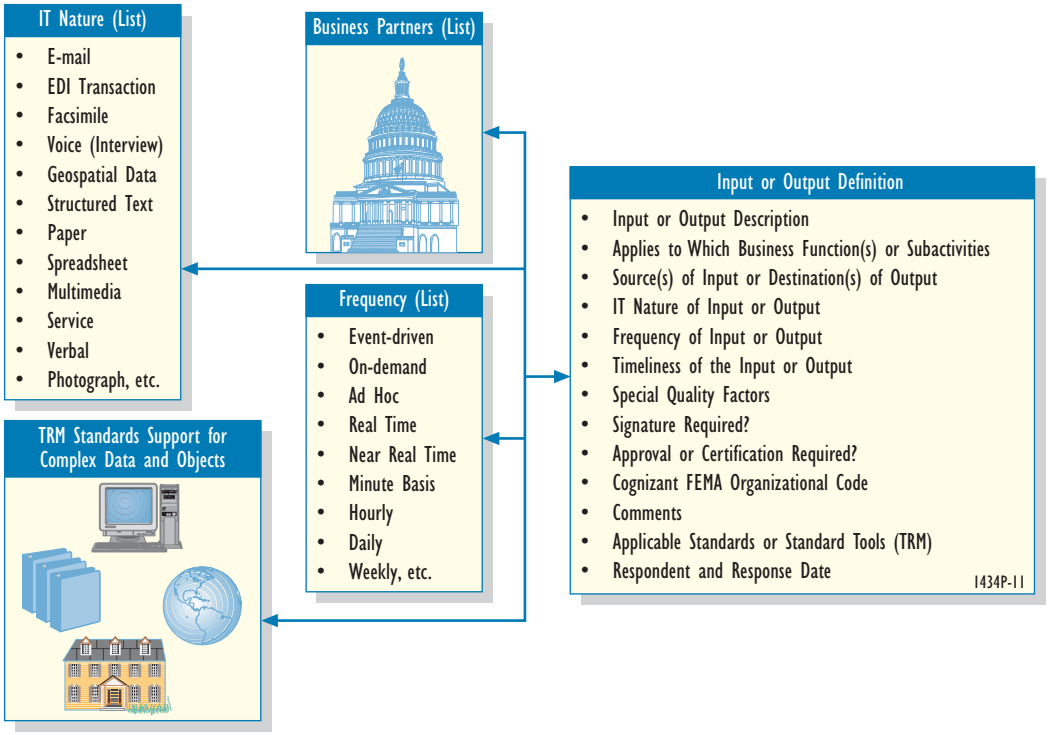


Figure 1-11. Scope of Structured Discussions on FEMA Information Flow Requirements

1.12.4.2 Identification of Major IT and Software Applications to Support FEMA's Mission

Within FEMA, IT applications and systems are categorized as either:

- Enterprise-wide systems
- Program-centric systems.

Enterprise-Wide Systems

As illustrated in Figure 1-12, one of the objectives of the target *FEMA IT Architecture* is to achieve well-integrated enterprise-wide systems and services.

Listed below are the major FEMA enterprise-wide applications, with a brief description of the application. A more detailed description and discussion of the business functions the application supports and of the standard tools the application uses are provided in Appendix M. Enterprise-wide applications are:

- **National Emergency Management Information System (NEMIS).** NEMIS will serve as a major application within e-FEMA. NEMIS is an integrated system to provide FEMA, the States, and certain other Federal agencies with automation to perform disaster and non-disaster operations. NEMIS requirements support all phases of emergency management, from State mitigation planning to situation assessments, providing disaster assistance, command and

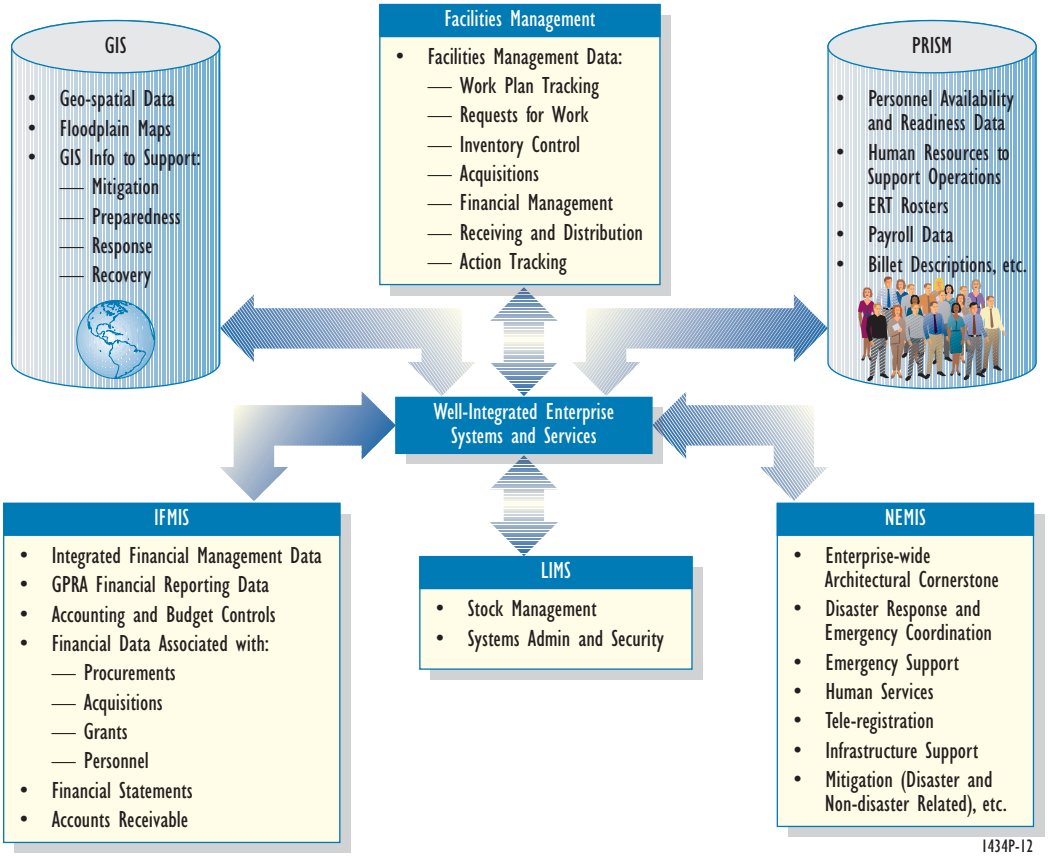


Figure 1-12. Target Architecture for Well-Integrated Enterprise-Wide Systems and Services

control, programmatic planning, emergency support, and mitigation operations. With the updated *FEMA IT Architecture, Version 2.0,* Automated Grants Management for both disaster and non-disaster are planned to be integrated with NEMIS. NEMIS provides users at all Region, Headquarters, State, and Disaster Field Office (DFO) locations with standard processes to support emergency management wherever a disaster occurs. It supports information resources that enable FEMA to integrate preparedness, situation assessment, PDA, and information and planning operations with FEMA programs and disaster assistance. This approach enables rapid and coordinated transition from monitoring an incident to managing declarations, setting up DFOs, and providing assistance to communities and individuals affected by a disaster.

FEMA Enterprise-Wide Geographic Information System (GIS). Within FEMA, GISs provide a good example of the opportunities and challenges of enterprise integration. Within FEMA, GIS is currently heavily used for floodplain mapping and insurance purposes. Data fusion from multiple sources, managed, and presented within an interactive GIS, can also support situation assessment and planning for the future evolution of a crisis. A representative example of current Map Analysis Center (MAC) GIS support for a hurricane consists of (1) executing a wind damage model prior to landfall and mapping probabilistic wind damage bands

to help determine the required scope of response; (2) integrating remote sensing data for damage assessment and assistance in response activity; and (3) geocoding disaster assistance application data and overlaying the data with sensing data for a combined view of the disaster. The MAC is currently developing an interactive mapping Intranet site that will provide desktop dynamic visualization of such maps and data.

In the future with distributed GIS available to States and local government via VPNs, a GIS map with building locations (drawn from a data base of residences and businesses) could be combined (for example) with sensor data on wind speed and direction to show where evacuation must take place. Integrating additional GIS-encoded data about the current location of emergency vehicles, shelters, evacuation personnel, and relief supplies could facilitate State/local evacuation planning and response and recovery functions for a wide scope of disasters. FEMA is in the process of establishing an enterprise-wide, integrated GIS capability to support mitigation; preparedness, training, and exercises; and response and recovery operations. This enterprise capability will assist in geographical data analysis, provide an interface to exchange GIS data within FEMA as well as external organizations, and serve as a maintenance medium for geospatial information. As previously mentioned, this process began with the formation of the FEMA GIS Working Group. The group is currently conducting an enterprise GIS requirements analysis and will also produce the subsequent enterprise GIS strategic plan and implementation plan. This is included in the Target Architecture Capabilities in this updated *FEMA IT Architecture, Version 2.0.*

- **Personnel Resources Information Systems Mart (PRISM).** FEMA's Office of Human Resources Management (OHRM) manages a set of personnel information systems that can be viewed as an enterprise-wide human resources data base. These IT systems include the Automated Deployment Data Base (ADD), a payroll system, a standalone COTS automated classification system (COHO), and a standalone COTS automated knowledge-base for management of employee conduct and performance (CHINOOK). There is connectivity to several other systems and data bases (e.g., OPM, Department of Labor, National Finance Center, and Treasury). PRISM, within the Target Architecture Capabilities in the updated *FEMA IT Architecture, Version 2.0,* is planned to be composed of data relative to processing personnel and payroll actions, reporting time and attendance, recording availability of personnel and tracking their assignments to disaster operations. It will also provide data to other FEMA organizational components through manual file transfers, including historical information for up to one year. With appropriate security access controls and privacy considerations, information within PRISM will be integrated with financial management data to form a more complete resource information data base and management reporting system with archival capability for up to six years. Further development of PRISM could include interface with other enterprise-wide systems, automated timekeeping, workforce management, automated requesting and tracking of personnel action requests, and executive and managerial information systems to include use of electronic signatures.

- **Logistics Information Management System (LIMS).** LIMS is FEMA's automated agency-wide property management and logistics information management system. LIMS is being re-engineered and will be compatible in architecture with NEMIS. The future re-hosted system (LIMS 2000) will support personal property management agency-wide:

— Property management
— Inventory control
— Financial interface to IFMIS.

- **Integrated Financial Management Information System (IFMIS).** Financial management is an important business function associated with both disaster and non-disaster operations. It is a particularly important function to management of FEMA's grants program with requirements to link financial reporting to performance measurements under GPRA. IFMIS was originally acquired from a software vendor. With re-hosting and re-engineering, IFMIS has become FEMA's enterprise-wide, financial management support system. The Office of Financial Management (OFM) has the responsibility for the development of IFMIS and its integration across the enterprise. IFMIS is the central component for achieving OFM's objectives to:
  — Improve financial management systems
  — Implement GPRA reporting
  — Issue accounting standards and financial statements
  — Develop human resources within the OFM
  — Improve management of receivables
  — Ensure management accountability and control
  — Modernize payments and business methods
  — Improve administration of Federal assistance programs
  — Manage and administer the disaster relief fund.

- **Facilities Management System.** This will be FEMA's system for facilities management support at Mt. Weather. It is intended to evolve into an enterprise-wide system and to be integrated with NEMIS through the use of COTS products. (Note: There are a series of integrated systems in use at the National Emergency Training Center [NETC] that serve the same purpose as this system. The NETC systems and this system were the basis of a needs analysis that led to procurement of a COTS facility management package that will be an enterprise system.) The Facilities Management System has the following functional requirements:
  — Work plan tracking
  — Requests for work
  — Inventory control
  — Acquisitions
  — Financial management
  — Receiving and distribution
  — Action tracking.

Program-Centric Applications

The number of these applications and systems is conservatively estimated at over 100. Appendix D provides a catalog of the program-centric systems. The current FEMA program-centric systems and applications manage, track, report, and maintain business information to support individual organizational elements' specific missions and business functions. With some exceptions, program-centric systems are characterized as small in volume of information. In general, they support specialized business functions. Examples include a system to generate and manage FEMA identification badges and an automated forms management system for developing, filling out, and routing forms electronically around FEMA.

As the target *FEMA IT Architecture* evolves and IT services are adopted, developed, and integrated as enterprise-wide, common, and re-usable architectural components, it is anticipated that there will be some consolidation or elimination of program-centric systems. As illustrated in Figure 1-13, the architectural goal is to have a manageable set of program-centric systems to create, manage, and use documents and data across the enterprise.

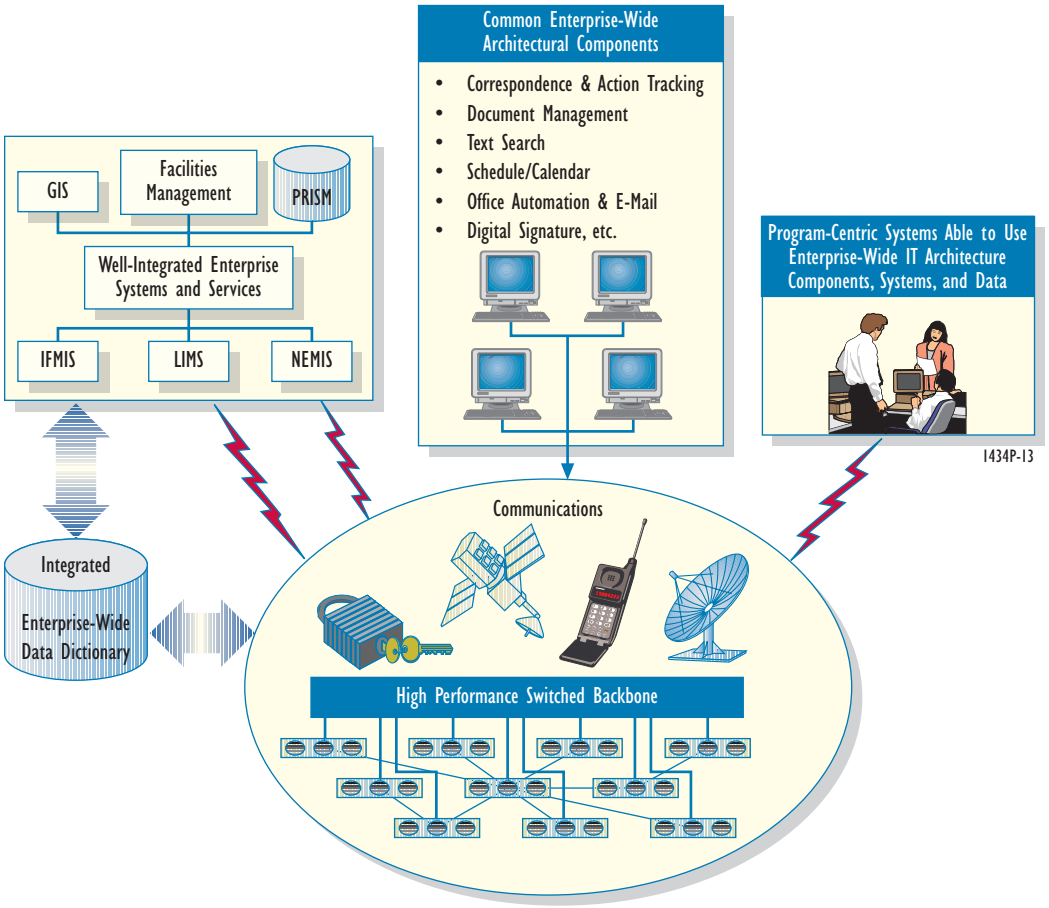
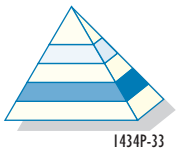


Figure 1-13. Architectural Concept for Integrating Program-Centric Systems

1.12.5 FEMA Data Descriptions

1.12.5.1 Introduction



This section of the *FEMA IT Architecture* addresses the FEMA high-level approach to data and document modeling. It explains how data is maintained, accessed, and used, from a data modeling perspective. The *FEMA IT Architecture* firmly establishes that data and document representation mechanisms are important for identifying information that can be shared across the enterprise, for minimizing redundancy, and for supporting new systems and applications. As the *FEMA IT Architecture* continues to evolve, FEMA will gradually move toward a robust object-relational modeling approach.

1.12.5.2 Identification of FEMA Documents and Data Stores

The structured interview process identified a large number of documents and data stores that are currently maintained as either enterprise-wide information resources or as program-centric resources. This was accomplished by analyzing:

- Major business functions assigned to FEMA organizational elements
- Key information flows (internal and external to FEMA)
- Categories of data and documents contained in, or managed by, various FEMA systems and applications.

Appendix G provides the results of that analysis. Appendix G lists the major documents and data stores maintained by FEMA Directorates and Administrations.

1.12.5.3 Major IT Architectural Characteristics of Current Documents and Data Stores

The following list briefly summarizes the major IT architectural characteristics of current FEMA documents and data stores:

1. **A significant number of documents within FEMA are received, processed, and managed as paper.** Examples include documents received via mail or fax, as well as documents that are photocopied and disseminated around the Agency. Frequently, these documents must be physically signed for authentication and legal purposes.

2. **Paper-based correspondence is sometimes scanned and managed as images,** but this is not universally accomplished across FEMA. Comparatively little of the material that is scanned is converted to intelligent form via optical character recognition (OCR) techniques. The few documents that are OCRed are not indexed with a text search tool.

3. **Most of the documents that are in electronic form within FEMA are developed, received, and maintained as office automation files.** These include word processing files, Portable Document Format (PDF) files, presentation graphics, and spreadsheets. Examples

of these types of documents include plans, policies, procedures, briefings, and reports. In general, the documents are not searchable and retrievable across the enterprise via an Intranet-based document management service. An exception is the comparatively few documents accessible on the FEMA Web site. A common form of interchange of electronic documents is as e-mail file attachments, though this approach is sometimes problematic due to occasional differences in sender and receiver e-mail systems. Generally speaking, this approach is a bigger problem for interchange of documents (as file attachments) with FEMA's external business partners.

4. **Comparatively few of the electronic documents that are created and/or interchanged (internally and externally) are in a structured format** with explicit content and structural tagging that would facilitate automated methods of routing and workflow management. Some structuring of word processing documents is loosely accomplished via templates, but this structuring is not universally accomplished and the authors can diverge from the template. Another exception is Web documents that are structurally-tagged using HTML but that are largely used for one-way information dissemination only.

5. **Virtually all of the documents that are created and/or interchanged are as *unitary files*, not as collections of objects** in an Object Linking and Embedding (OLE) sense. While this approach facilitates document management as standalone files, it does not adequately support the storage and intelligent re-use of embedded objects in the documents such as graphics, multimedia objects, and other entities such as spreadsheets and organization charts.

6. **From the point of view of automated transaction processing, FEMA does some Electronic Data Interchange (EDI)** with suppliers, vendors, and partners. However, much of this interchange is done in a point-to-point manner using customized or non-standard data transfer protocols, as opposed to ANSI X12 transaction sets, which are an open systems standard.

7. **Many of the program-centric systems and applications that have been developed use Microsoft Access as the data base management system of choice.** Access is accepted as an enterprise-wide standard tool for desktop data base efforts. Because these data bases are maintained locally, they are not accessible via on-line means across the enterprise.

8. **Within FEMA, increased emphasis is being placed on enterprise design and modeling of documents and data stores, and on standardization using Oracle.** Examples of this activity include structuring of documents and data in projects such as the enterprise-wide GIS, IFMIS, LIMS, Facilities Management System, and NEMIS. NEMIS, in particular, has developed an approach to logical and physical data modeling which is currently adopted as the FEMA enterprise-wide standard data modeling approach. Within NEMIS, data and document representation mechanisms have proven useful for identifying information that can be shared across the enterprise, for minimizing redundancy, and for supporting new applications. With this attention to detail, more and more FEMA enterprise information is beginning to be represented in an intelligent format and to be interchanged via direct computer-to-computer data base transactions. An excellent example is the tele-registration component of NEMIS that supports vital human services needs during a time of crisis.

Furthermore, this attention to detail is leading to increased re-use of documents and data, as well as improved document and data integrity. As the *FEMA IT Architecture* continues to evolve and as tools are identified, it is anticipated that the current entity-relational modeling approach will mature to a more robust object-relational modeling approach.

1.12.5.4 FEMA Approach to Enterprise Data and Document Modeling

From a *FEMA IT Architecture* perspective, NEMIS implemented an enterprise-wide, standardized approach to data modeling using PowerSoft's S-Designor Computer Aided Software Engineering (CASE) tool (now called PowerDesigner). The current NEMIS entity-relational approach to enterprise-wide data modeling is described in more detail below.

Figure 1-14 provides a sample of the logical data model that was developed for the Emergency Coordination (EC) component of NEMIS. The NEMIS enterprise data models were developed in due consideration of FEMA's mission and major business functions. The NEMIS data models promote sharing of information across the enterprise and the elimination of redundancies. NEMIS has developed and documented comprehensive data models for the following:

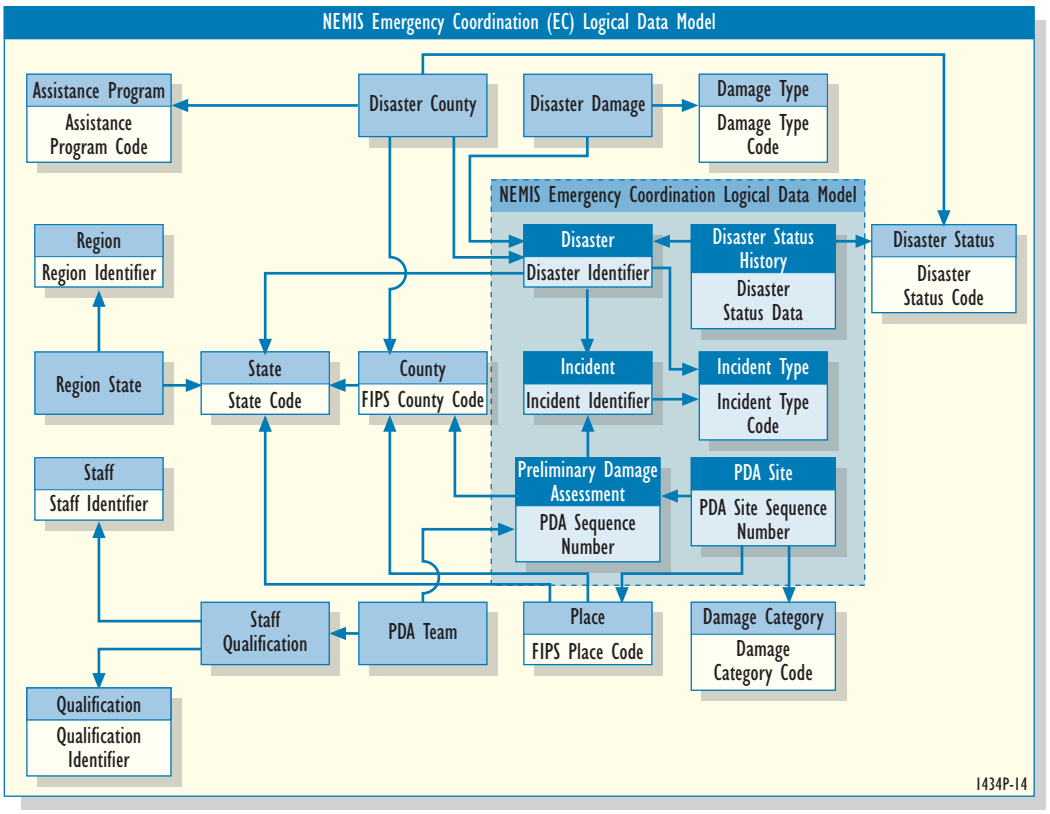


Figure 1-14. Sample NEMIS Logical Data Model

- Human Services (HS)
- Infrastructure Support (IS)
- Mitigation (MT) (disaster and non-disaster)
- Emergency Coordination (EC)
- Emergency Support (ES).

Within NEMIS, the data models include the following major components:

- **Logical Data Model.** The logical data model specifies the data structures and business rules needed to support a business area without consideration of the hardware or software that will be used to implement it. The logical data model indicates those entities that have been identified as occurring in more than one functional area, thereby promoting enterprise sharing.

- **Physical Data Model.** The NEMIS physical data model specifies the physical implementation of the data base showing all the tables, columns, and keys for the Oracle 7 relational data base. The physical data model also indicates entities that have been identified as occurring in more than one functional area.

- **Data Dictionary.** This portion of the NEMIS data modeling process contains the following reports:
  - **Entity Attribute Report.** The entity attribute report specifies in tabular format the name and definition for each data entity along with a list of all the data attributes associated with the entity. For each attribute, its corresponding data type and size are given along with an indication of whether it is a component of the primary key of the entity and whether it is a mandatory field.
  - **Attribute Report.** This report specifies in tabular format all the unique attributes in the model along with their characteristics, definition, and a where-used cross-reference.
  - **Oracle Data Base Schema.** The Data Base Schema is the actual script that is used to create all the tables, columns, indices, and referential integrity constraints for the Oracle 7 relational data base.

1.12.5.5 Integration of Documents and Data

Within the target *FEMA IT Architecture*, documents can be viewed as collections of data objects. Currently, most electronic documents within FEMA IT systems consist of unstructured word processing and office automation files. Consistent with the principle of creating documents in their most intelligent form, managing them over their life cycle, and then gaining maximum downstream re-use, FEMA is carefully moving toward a digital library concept where documents are intelligent, structured, and composed of re-usable objects. As this concept is gradually implemented, FEMA will migrate to a formal object-relational modeling approach. This object-relational approach is consistent with government and industry direction as part of the National and Global Information Infrastructure (NII/GII) initiative. The FEMA IT architectural approach is also facilitated by open systems standards such as SGML and XML, which are described in more detail in the Technical Reference Model (TRM). With strong industry support (e.g., Microsoft, Netscape, Oracle, and others), XML is intended to replace HTML as the preferred standard to represent and interchange complex documents on the Web. As illustrated in Figure 1-15, SGML

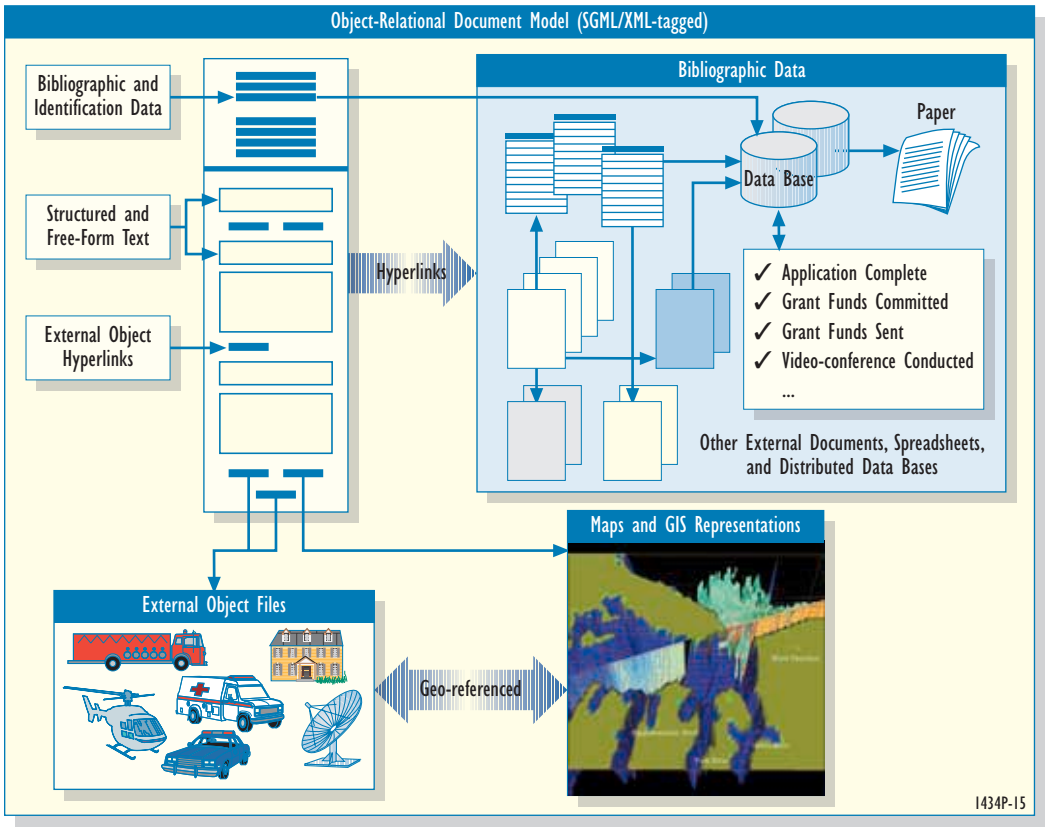
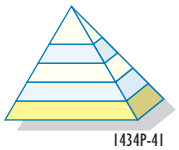


Figure 1-15. Integration of Documents and Data with an Object-Relational Document Model

and XML facilitate the structuring of documents and their linking with other documents, spreadsheets, and distributed data bases, maps and GIS representations, and external object files.

1.12.6 FEMA Technology Infrastructure

1.12.6.1 Introduction



This section of the *FEMA IT Architecture* identifies and describes the underlying IT infrastructure. The underlying technology infrastructure is described in terms of re-usable IT *architectural components* that provide functional capabilities and services that can be integrated into FEMA enterprise-wide and program-centric systems. Architectural aspects associated with the high-level *wiring diagram* of communications and networks are addressed in Section 3.

1.12.6.2 Principles for Enterprise Integration and Re-Use of Architectural Components

An *architectural component* is defined as a high-level building block or piece of a larger system that can be used and re-used across multiple systems in a cost effective and standardized manner.

Architectural components are sometime referred to as *middleware* or the basic building blocks of IT systems. Architectural components make up the basic FEMA IT systems and network infrastructure. Architectural components broadly include IT standards, hardware, networks, software, processes, environmental factors, partnerships and relationships, data stores, documents, common business function requirements, technologies, and tools that are used to build systems or that are used within a system.

This section identifies and discusses a number of common and re-usable IT systems and tools that have the potential to become standardized and re-usable architectural components. Consistent with the IT architectural model presented in Section 1.11, the technology infrastructure is intended to directly support FEMA's business processes.

Section 1.8 of this updated *FEMA IT Architecture, Version 2.0,* sets forth the architectural principle that: *"Any proposed IT development activity shall re-use existing defined enterprise-wide architectural components unless the components can be demonstrated to be inadequate to the requirements to the satisfaction of the CIO and the IRB."* This principle will help drive more cost effective systems development and is essential for achieving increased interoperability and standardization. It also provides a mechanism for highlighting any deficiencies in the definition or implementation of common architectural components across the FEMA IT infrastructure.

1.12.6.3 Leveraging Technology Developments in Other Agencies and Industry

The *FEMA IT Architecture* has a major goal of achieving increased interoperability with FEMA's business partners. FEMA seeks to leverage technology developments in other agencies and industry. FEMA will monitor the work of the CIO Council, industry groups, voluntary organizations, universities, and its business partners.

1.12.6.4 Identification and Synopsis of FEMA Enterprise IT Architectural Components and Services

Figure 1-16 depicts how a FEMA enterprise-wide system or a program-centric system could use and re-use common IT architectural components.

During the structured interview process, a significant number of organizational elements identified a common set of IT architectural needs that are identified in Figure 1-16.

1.12.6.5 High-Level Architectural Considerations

It is important to note that all of the IT services and needs identified in the structured discussions above are fairly generic and are not specified in detailed systems engineering or design terms. This statement reflects the fact that the purpose of the *FEMA IT Architecture* is to define a ***technology vision***, not a detailed systems engineering design. It makes good economic sense, and advances the objective of interoperability, for the FEMA ITS Directorate to design and develop these capabilities as common, enterprise-wide, standardized components. The programmatic intent is to develop standardized architectural components, which can be re-used across both

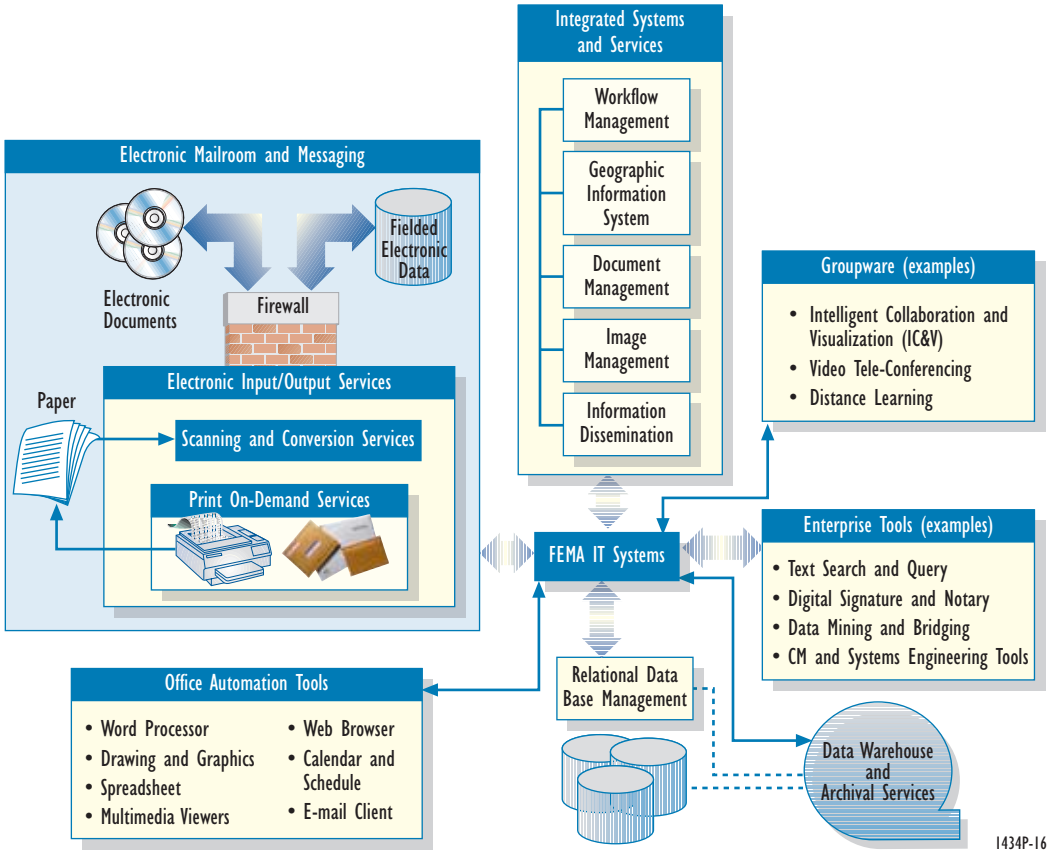


Figure 1-16. Identification of Re-Usable Architectural Components for FEMA IT Systems

enterprise-wide and program-centric IT systems. To the maximum extent practicable, FEMA also desires to leverage IT investments and technology insertion activities in other Federal agencies.

Need to Conduct Business Case Analysis Following the Capital Planning and Investment Control Process

Another important point to make at this juncture is that some of the architectural components and technology implied by Figure 1-16 require further analysis given the current state of FEMA networks and recent progress that has been made. For example, advanced groupware technologies such as intelligent collaboration and visualization; integrated voice, video, and data applications; distributed interactive simulation (DIS); and distance learning (incorporating VR technology) are widely accepted to be bandwidth intensive in large-scale distributed operations. The current FEMA network only has limited capability to support some of these advanced technologies today. Accordingly, it is important to realize that Figure 1-16 merely provides an architectural vision or framework for discussing **how** FEMA IT systems might be structured to use common architectural components. Business case analyses, included as a component of the Capital Planning and Investment Control Process (CPIC) required by OMB, for the more demanding architectural components clearly need to be accomplished before any actual imple-

mentation. FEMA is initially implementing its own process, the *IT Capital Planning and Investment Guide (CPIG)*, as an internal capability that is compatible with CPIC.

Need to Integrate with Security Architecture

Another important point is that IT architectural components need to be developed and integrated in consideration of a robust security architecture, which provides important services including confidentiality, data integrity, originator authentication, ensured service availability, and non-repudiation. FEMA is currently planning to initiate extensive security architecture work.

NEMIS as an IT Architecture Development Environment

FEMA notes that many of the desired capabilities and IT needs that were identified during the structured discussions are currently under development or are under active investigation by the NEMIS Project. Thus, NEMIS provides FEMA with an important IT architecture breeding, testing, and integration environment for a number of the concepts. The successes of NEMIS achieved during the past two years since the initial publication of the *FEMA IT Architecture, Version 1.0,* are discussed in the Executive Summary of this document.

Major Architectural Components

The remainder of this section briefly identifies and describes the major IT architectural components that were identified during the structured discussion process. This discussion follows the layout of Figure 1-16 and addresses the major elements. The architectural framework provides IT systems with access to the following:

- **Digital Library Services** includes access to distributed documents and data bases, data warehouse, and archives via an enterprise-wide relational data base management system (RDBMS). The current FEMA relational data base standard is Oracle. The latest release of Oracle is Oracle 8. Oracle 8 is an object-relational data base management system, which provides improved handling of large objects typically seen in a distributed digital library environment.

- **Integrated Enterprise-Wide Systems and Services** such as workflow, GIS, DMS, Image Management System (IMS), and information dissemination services.

- **Bi-Directional Electronic Mailroom and Messaging Services** including 24-hour per day and 7-day per week (24/7) support for print on-demand and mail; scanning and conversion of paper-based documents; and electronic input/output (I/O) services for processing, handling, validating, and receipting of electronic documents and fielded electronic data transactions.

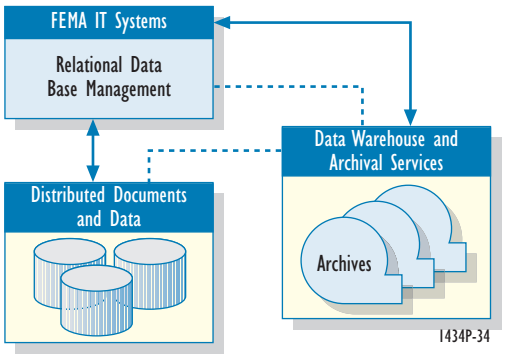
- **Office Automation Tools.**

- **Enterprise-Wide Standard Tools** such as text search, digital notary, data mining, print on-demand, rendering and display, etc.

- **Groupware.** Within this *FEMA IT Architecture*, groupware is broadly defined as software or middleware that facilitates intelligent collaboration and visualization activity on digital library objects distributed across the enterprise. Groupware may take advantage of enterprise tools, distributed

data and documents, applications, models and simulations, mailroom and messaging services, etc. In reference to Figure 1-16, groupware might also support a Java-based Web interface.

1.12.6.6 Digital Library Services



The target *FEMA IT Architecture* provides for development of digital library services managed by a RDBMS. At the current time, NEMIS digital library services are mostly text-based.

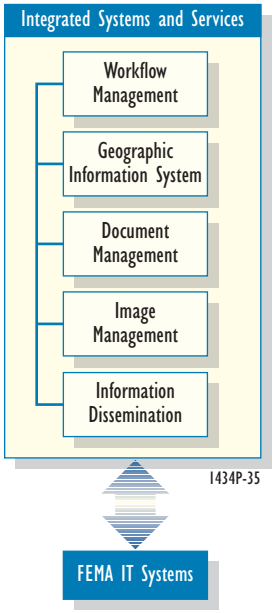
Based on structured discussions with FEMA organizational elements, a potential requirement exists to extend digital libraries services to manage other complex objects, including mixed-mode compound documents and data sets (e.g., hyperlinked text, images, graphics, multimedia, spreadsheets, interactive GIS, etc.) as illustrated in the data model shown in Figure 1-15. This effort may require migration in the future to an object-relational data base management system such as Oracle 8.

The digital library support services also need to consider providing support for a data warehouse and archives for legal and regulatory purposes as well as backup and recovery. Special attention will need to be placed on services to maintain long term document and data integrity within the digital library. Also, with NEMIS as the organizational lead, FEMA will strive toward standardization and harmonization of enterprise-wide data dictionaries.

As the FEMA network evolves with improved Quality of Service (QoS), the digital library can become more interactive and can be integrated with groupware services such as integrated voice, video, and data applications; distributed planning tools; and distance learning tools. Development of robust and effective digital library services across the enterprise will need to carefully consider integration of other architectural components such as correspondence and action tracking, document management, image management, electronic mailroom and legacy data capture, multimedia, and text search components. Correspondence and Action Tracking is now included as a new project in FEMA's Target Architecture Capabilities in this updated *FEMA IT Architecture, Version 2.0,* and is discussed in detail in Volume 2, Appendix P, of this document.

1.12.6.7 Integrated Enterprise-Wide Systems and Services

Integrated enterprise-wide systems and services represent a class of COTS products and services that manage and control various classes of documents and data sets. In general, these systems and services need to be closely integrated with an enterprise RDBMS through the use of Application Program Interfaces (APIs). An advanced Document Management System (DMS), for example, is used to create and manage documents as collections of objects (e.g., text, graphics, and multimedia). These objects form part of the digital library that is managed by an RDBMS. The structured interviews identified several potential enterprise-wide systems and services. These systems and services include:



- **Workflow Management.** NEMIS has used Viewstar for workflow services. However, the implementation has not been as successful as desired. Enterprise-wide automated workflow services integrated with a document management capability are typically needed in document-related and repetitive applications such as grant management and correspondence and action tracking. Workflow processes can also support repetitive mailroom services such as receipting, validation, and routing of documents, as well as print on-demand approaches for information dissemination. Enterprise-wide workflow services were a commonly cited requirement in the structured interviews and can be applied in repetitive business functions.

- **Geographical Information System (GIS).** Tighter integration of GIS with FEMA's business functions was cited by nearly every FEMA organizational element as being important to FEMA's mission. GIS systems provide specialized capability to manage and link geospatial data, as well as provide tools that lead to an increased understanding of the underlying geographical factors associated with FEMA's operations. Important objects in crisis management scenarios and mitigation activities can be geo-referenced, indexed, and searched within a GIS. See Figure 1-15 for the concept. From an IT perspective, the FEMA standard GIS products are MapInfo Professional and ARC/INFO. As the *FEMA IT Architecture* evolves and the network is enhanced with QoS and improved bandwidth management provisions, the potential exists to make the FEMA enterprise-wide GIS be more accessible to FEMA's business partners and to be much more interactive for very large and complex maps. As the GIS is better integrated with models and simulations, it will be better able to support mitigation, response and recovery, as well as preparedness, training, and exercises. In addition, the requirement for a spatially enabled Oracle RDBMS is inherent within this enterprise GIS concept. As previously stated, FEMA, through the GIS Working Group, is currently undertaking the effort of planning the enterprise GIS by conducting a requirements analysis and developing the subsequent strategic plan and implementation plan. The updated *FEMA IT Architecture, Version 2.0,* now includes GIS enterprise integration in the Target Architecture Capabilities, which are discussed in Appendix P in Volume 2 of this document.

- **Document Management System (DMS).** In general, there are four classes of DMSs. These classes include:
  - — DMSs that treat and manage documents as scanned images. These DMSs are frequently referred to as Image Management Systems (IMSs). Within the *FEMA IT Architecture*, this class of DMS is addressed in more detail below.
  - — DMSs that treat documents as single unitary files such as word processing files with embedded images.
  - — DMSs that treat documents as collections of discrete objects, but that manage the text stream as a single file with external links to objects such as graphics and multimedia.
  - — DMSs that treat documents as collections of objects with links to external objects such as graphics and multimedia and that manage the text stream as discrete elements with discrete tagging or markup using SGML, XML, or HTML. These DMSs can potentially treat

individual elements such as paragraphs, chapters, titles, hyperlinks, tables, and even cells within a table as discrete, manageable objects. These types of DMSs are referred to as *fine-grained* DMSs and are most frequently employed in digital library systems. This class of DMS is recommended and is generally capable of handling unitary files and simpler object models of documents. From a commercial perspective, this class does not usually support image-based models of documents.

A significant number of the structured interviews identified an enterprise-wide DMS as a potential need within FEMA. A DMS integrated with workflow, text search, the enterprise RDBMS, digital signature (if needed), display and rendering tools, office automation products, e-mail and messaging services, and scanning and conversion services forms the essential ingredients needed for development and integration of (1) Correspondence and Action Tracking System and (2) an Automated Grants Management System. Both of these systems are now included in the updated *FEMA IT Architecture, Version 2.0,* Target Architecture Capabilities. These systems are discussed in detail in Volume 2, Appendix P, of this document.

- **Image Management System (IMS).** In general, IMSs treat documents as scanned collections of pages. Within FEMA, image management is important because a significant number of documents are still received in paper format. IMSs have the advantage of preserving the *look and feel* of the original document, albeit as a facsimile. An image-based system also preserves any handwritten signature within the image. The major disadvantage of image-based DMSs is that the documents are not intrinsically searchable using text search tools without applying OCR techniques, which tend to be inaccurate and which must be quality controlled. Given the large volume of paper-based and facsimile documents that FEMA receives, the *FEMA IT Architecture* recommends incorporation of an IMS. The IMS should be integrated with scanning and conversion services within an electronic mailroom. The IMS also needs to be integrated with other elements of the digital library including the enterprise RDBMS, the intelligent DMS, workflow services, and text search services (for OCRed documents).

- **Information Dissemination Services.** The structured interviews indicated that information dissemination is an important service for FEMA for mitigation support and for public notification during response and recovery operations. Information dissemination also supports preparedness and is needed in such areas as floodplain insurance for marketing purposes and fire administration for dissemination of fire incident reports and lessons learned. The *FEMA IT Architecture* recommends development of common information dissemination services as an enterprise-wide architectural component. The information dissemination services need to be fully integrated into the digital library services. Other integration should include interface with Java-based Web interfaces that support streaming audio and video (push-pull technology), the RDBMS, the DMS and IMS, the data warehouse, workflow (for scheduled information dissemination releases), electronic mailroom and messaging services, groupware, and text search tools.

1.12.6.8 Bi-Directional Electronic Mailroom and Messaging Services

A key component of the proposed *FEMA IT Architecture* will be 24/7 support for bi-directional electronic mailroom and messaging services. These services will provide for the receipt, distribution, and dissemination of information including a broad scope of documents and data. Bi-direc-

tional electronic mailroom and messaging services are an essential element of correspondence and action tracking. This paragraph defines the major architectural components that are currently anticipated to be needed for an electronic mailroom and messaging services. As such, they provide a high-level architectural vision.

Within FEMA, the IRB has established a task force to review current systems including NEMIS, ACTS, the Correspondence and Issues Management System (CIMS), and others, which either use and/or provide electronic mailroom services in support of correspondence and action tracking. The task force will generate and refine requirements covering Agency needs in the combined areas of action tracking, correspondence control, and document management. The group will also review processes (such as mailroom services) that are necessary to implement an enterprise-wide correspondence and action tracking system. In addition, the Executive Secretariat had an independent review performed on the Agency's correspondence and actions tracking processes.

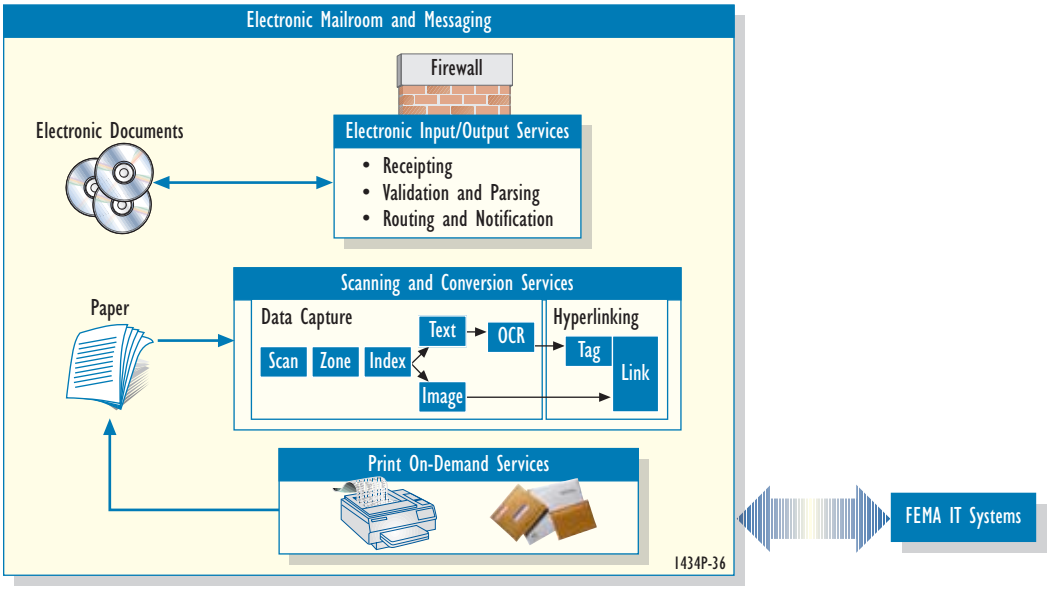
The products of the IRB task force will consist of a requirements document, a process document, and recommendations on software solutions. The ITS Directorate will provide support to the group for reviewing existing products, specifically NEMIS and ACTS. The Directorate will also generate specific IT requirements, review other COTS software solutions, conduct cost/benefits analysis, and prepare life-cycle cost estimates. The Operations Support Directorate will provide the lead on process recommendations. The electronic mailroom and messaging services described below are intended to provide high-level architectural inputs to the IRB task force and are subject to further refinement.

The results of the IRB work, and the Executive Secretariat's report, helped contribute to the need to include correspondence and action tracking as a new project in FEMA's Target Architecture Capabilities. This is discussed in detail in Volume 2, Appendix P, of this document.

Electronic Input/Output Services, Scanning and Conversion, and Print On-Demand Services

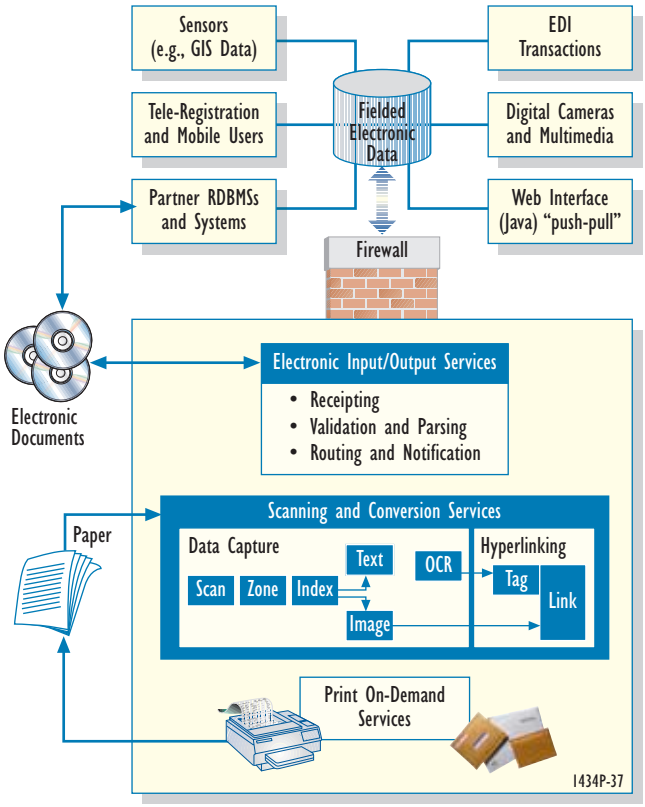
The three major components of the 24/7 bi-directional electronic mailroom and messaging services include:

- **Electronic Input/Output Services.** The electronic receipt and dissemination of information under the *FEMA IT Architecture* includes basic services for processing structured electronic documents and fielded data. When an electronic document is received at the electronic mailroom, a receipt may be sent back to the document originator via e-mail or other electronic means to acknowledge the transaction. If the document is in a structured format such as SGML or XML, the document is parsed under software control to ensure that the document instance conforms to the document model it was created under. At this time, any external objects, such as graphics files, can be checked to ensure that they are readable. Once the document is validated, it is handed off to the DMS or IMS as appropriate for cataloging and check in. At this point, if the recipient is known, the workflow management system is invoked to route the document to the intended recipient. The electronic I/O services also support validation of fielded electronic data and messaging to authorized external users, customers, and the public through appropriate security measures and firewalls.



- **Scanning and Conversion Services.** Because documents received by FEMA will continue to be sent in paper format for the foreseeable future, the proposed technical architecture will include provisions for converting them into digital format. The first step in this process is the actual scanning of the document into an image-based format. From here, the document may take one of two paths. The first path is for documents that will be stored in image format. These documents are simply scanned and indexed before being routed into the IMS. A good example of this process is the current approach used in CIMS. The second, more complex path is used for documents that are to be converted into an intelligent format for later re-use. After the initial scanning to image format, these documents are processed by OCR software to recover the actual text and format of the document. At the same time, any graphical material is saved to an image format and linked to its location in the text stream. If the document is to be converted to a structured information format, as illustrated in Figure 1-15 (e.g., HTML or XML for Web-based delivery), autotagging software applies the necessary markup to the text file and links any graphic objects as separate files. From here, all documents are routed to either the IMS or DMS, depending upon the format. The automated workflow component is then invoked to route the document to the proper place and to process repetitive events such as action tracking, grants management, etc.

- **Print On-Demand Services.** The final component of the digital mailroom is the print on-demand component. Print on-demand functionality allows users to create hardcopy for information dissemination purposes. As indicated in the TRM, the FEMA standardized approach for print on-demand uses Xerox DocuTech and DocuColor. This function also supports such services as direct mail and marketing support (e.g., automated mailing list distribution of Federal Insurance Administration materials).



Support for Direct Bi-Directional Data Transfer of Fielded Electronic Data

As illustrated, with appropriate security and firewall provisions, the electronic mailroom and messaging services can provide an architectural framework and interface for bi-directional data transfer of fielded electronic data. The interchange of fielded electronic data is functionally different from the interchange of structured electronic documents in that the interchange can be under the direct control of a relational data base management system (RDBMS).

With appropriate wide-area security and firewall considerations addressed, examples of the use and interchange of fielded electronic data might include the following:

- **Web Interface (Java).** Java-based Web interfaces can be developed and integrated with information dissemination services and the digital library to support information *push-pull* concepts including streaming audio and video. The Java-based Web interface can also support distributed groupware applications such as distance learning, distributed planning, and intelligent collaboration and visualization. Java-based interfaces can also be developed to support mobile users and authoring and validation of documents such as grant applications.

- **Electronic Commerce (EDI and EFT Transactions).** Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT) are two classes of structured or fielded data interchange that can be handled within this architecture.

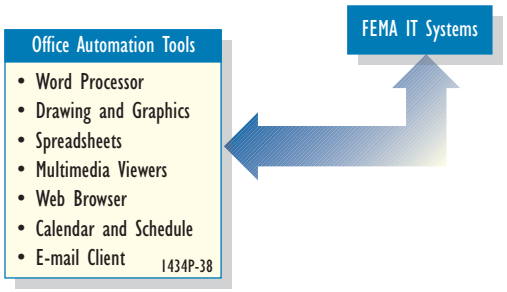
- **Tele-Registration, Mobile Users, and Information Kiosks.** When integrated as part of an IT system such as NEMIS, the Electronic Mailroom and Messaging services can directly support fielded data transfer as well as document transfer and digital library services to remote users. Tele-registration is an excellent example of direct computer-to-computer fielded data transfer that is incorporated within NEMIS. With validation and messaging notification, the concept of direct fielded electronic data and document interchange can readily be extended to mobile users and information kiosks.

- **Systems for Sensory Data (e.g., for GIS applications), Digital Cameras, and Multimedia Capture Devices.** Many IT systems produce fielded or structured electronic data for sensors,

digital cameras, and multimedia data capture devices. With appropriate security and firewall considerations, the electronic mailroom and messaging services can support a direct interface with these systems. With input and output validation services and receipting, the electronic mailroom can serve as a high-level architectural interface to receive and process GIS data from external sources. In that the fielded electronic data interface to systems is anticipated to be bi-directional, the potential exists within this high-level architecture to support advanced concepts such as tele-presence and other collaborative techniques.

- **FEMA Business Partner RDBMSs and IT Systems.** With appropriate security and firewall provisions and with carefully crafted Memoranda of Agreement (MOAs), the high-level architecture for electronic mailroom and messaging services can support direct electronic document and data transfer with FEMA's business partners. Additional IT architectural work needs to be accomplished to design, develop, and implement networks such as Extranets and Virtual Private Networks (VPNs). Security technologies such as Kerberos token passing for originator authentication need to be more actively explored. Also, criteria will need to be developed to support receipting of information, validation and parsing of the data and documents, and routing to appropriate individuals and IT systems. With the integration of groupware concepts such as intelligent collaboration and visualization and distance learning, it should be possible in the future to extend digital library concepts (including GIS data) to FEMA's business partners, as well as have FEMA be able to access data and documents within external systems. This extension will need to consider the potential impact on FEMA network bandwidth management.

1.12.6.9 Office Automation Tools



As illustrated, FEMA IT systems and users need to be able to exploit current and evolving office automation tools. Many of the documents and data sets that FEMA produces are appropriate for authoring using COTS office automation products, such as Microsoft (MS) Office and MS 2000.

Within MS Office, file formats are acknowledged to be proprietary and require additional profiling to meet archival storage requirements. Future needed office automation capability includes:

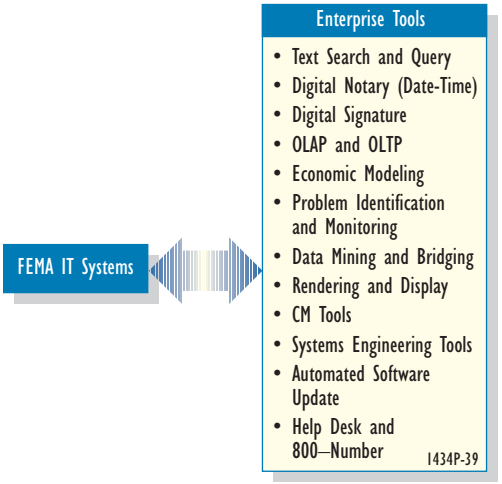
- **Authoring of XML** (as an open systems replacement for HTML on the Web) consistent with the object-relational document model as shown in the Figure 1-15 data model. XML is expected to be in the next release of MS Office. Other SGML and XML tools are widely available. Document Type Definitions (DTDs) and style sheets for structured documents need to be developed, standardized, and coordinated across the enterprise.

- **Authoring, Use, and Enterprise-Wide Integration of Electronic Forms on the Desktop.** Jetform Formflow is under consideration and evaluation by the Operations Support Directorate. Jetform is used by many other Federal agencies, thereby promoting interoperability. The proprietary file format needs to be profiled and defined to promote it to archival status.

Components of the current FEMA office automation tool kit include:

- Word processor (Word)
- Spreadsheet (Excel)
- Presentation graphics (PowerPoint)
- Desktop RDBMS (Access)
- E-mail client (Exchange Server and Outlook)
- Web browser and plug-ins (Internet Explorer)
- Web page authoring (Word augmented by FrontPage)
- Calendar tool (scheduling) (Schedule+)
- Contact manager (Schedule+ and Outlook)
- Task manager (simple) (Outlook)
- Journaling tool (Outlook)
- Windows environment (NT, Win 95/98)
- Multimedia playback (Media Player).

1.12.6.10 Enterprise-Wide Standard Tools



A key feature of the proposed *FEMA IT Architecture* illustrated in Figure 1-16 is the availability of enterprise-wide, standardized software tools working in a secure environment. These tools provide key capabilities for accessing, manipulating, managing, and using the broad range of information available in the FEMA IT environment. Each of these tools provides certain functionality in the IT architectural plan. NEMIS is addressing many of these tools.

The following list summarizes the major capabilities and requirements that were identified in the structured interview process:

- **Text Search and Query.** State-of-the-art text search tools allow users to identify and retrieve mission-critical information across heterogeneous data and document sources. Users can query the data collection in a distributed environment without knowing the actual data sources physical location. Queries can be constructed and stored for later use or repetitive searching requirements. Queries themselves can be built upon key word indexing and query constructors (e.g., and, or, not, etc.), fuzzy logic matching, and tailored indexes. Advanced searches can employ artificial intelligence techniques to find relevant information based upon semantic similarity. Periodic indexing of the data and document collection takes place as a background task in order to ensure rapid response as the data collection grows. NEMIS has utilized Oracle ConText as a text search tool. The requirement for an enterprise-wide approach to text search and retrieval was among the most frequently cited requirements during the structured interview process.

- **Digital Notary.** An important concern for digital documents in a future electronic commerce environment is the need to ensure that unauthorized changes cannot occur without detection. Digital notary services such as those provided by Surety Systems and other services such as secure board-level clocks from Datum, Inc., can provide this level of assurance. In the Surety model, the digital notary service generates a secure hash based upon the content of the document or file and combines this hash with other hashes received from other documents processed at the same time. The approach not only locks the content of the document but also securely date-time stamps it. If the document or file is changed in any way, the digital time stamp no longer matches, and the document is flagged as altered by the notary service client software. The rolling time hash is published in a major periodical as a form of public witnessing, further ensuring that no compromises can be made to the file content.

- **Digital Signatures.** The need for secure digital signatures was a commonly expressed requirement during the structured interview process, though there was some misunderstanding about a raster-scanned signature as being a digital signature. With the implementation of GPEA by October 2003, FEMA is required to consider the enterprise-wide integration of digital signature services where practicable. A prior concern was that digital signatures were not well integrated and supported as a widely implemented component of the e-government infrastructure. GPEA implementation will lead to progress in this regard. A widely-recognized major concern is binding the public key of the sender of the information to the particular individual. Also, FEMA has concerns about standards and interoperability as well as cost. Nonetheless, in an electronic environment, in the absence of paper-based representations for documents, a reliable mechanism for representing signatures is required. In the digital environment, this mechanism must be able to authenticate a signer relative to a specific file or collection of files. Public key encryption provides this service by using a pair of unique digital keys. The first key is a private key used by the party signing the document. The second key is a public key known to the document recipient and bound to the sender via some recognized certificate authority. The private key is used to generate a unique hash file based upon the file content being sent and the key value itself. The signature hash file is then sent with the document file to the recipient. The public key is used by the recipient on the signature file to authenticate the sender and the file content. The digital signature approach can be combined with date-time stamping. FEMA will evaluate these issues associated with digital signatures in GPEA implementation.

- **On-Line Analytical Processing (OLAP) and On-Line Transaction Processing (OLTP).** OLAP and OLTP are comparatively new services that are of interest to organizations such as OFM and the Federal Insurance Administration . These services provide users with advanced capabilities for search and information retrieval in the distributed computing environment. These processes act as intelligent agents that continually monitor the distributed data sources for information on a particular topic, such as losses or claims on a set of insurance policies. These processes work in the background without user intervention and report items of interest when they are found. This capability can be an extremely powerful tool for monitoring such things as information on a particular geographical region of the country, claims on an insurance policy, aggregated grant management performance results, a particular type of disaster, or a certain subject of interest.

- **Economic Modeling Tools.** Economic modeling tools will allow FEMA managers to better estimate costs by modeling financial data in a way that best represents the problem area. Flexibility built into these tools will allow alternatives to be compared and different scenarios to be run to assess economic impact. Simulation capabilities will also allow causal relationships to be identified in the data that might otherwise remain undetected.

- **Problem Monitoring and Tracking Tools.** Within the target *FEMA IT Architecture*, there is a need for automated tools to help identify and track events related to a particular problem or situation. Problem monitoring and tracking tools can be potentially standardized as common architectural components. These tools, combined with the OLAP and OLTP services previously mentioned, can potentially provide FEMA personnel with a reliable and up to date source of problem information. These tools can allow the users to gather, organize, sort, annotate, and present information in a manner best dictated by the particular problem or situation. Information collected may come from a number of disparate sources and in varying data formats. These tools will allow the users to collect, analyze, and use this information quickly and accurately.

- **Data Mining and Heterogeneous Data Base Bridging Tools.** The need for an enterprise-wide ability to support data mining and bridging of heterogeneous distributed data bases was expressed by a significant number of respondents during the structured interviews. Data mining tools are software that sifts the data and looks for new patterns, trends, and relationships. In principle, they can be applied across internal and external data bases and are an important architectural component for digital library services. As the GIS data library grows, there is significant potential to apply data mining technology to support mitigation activity. Data mining can also be applied to identify trends in exercise results. Data base bridging is a technology to support queries and joins across heterogeneous data bases. Heterogeneous data base bridging tools basically accommodate unique syntactic and semantic differences in various data base vendor implementations of Structured Query Language (SQL). The tools are also useful in harmonizing differences in data dictionaries across various data base implementations.

- **Rendering and Display Tools.** Because the target *FEMA IT Architecture* will contain many different types and formats of information, tools must be provided for presenting the information in human-friendly terms. The IT toolkit will provide users with a number of rendering and display tools for this purpose. Standardized tools need to be developed or acquired to render textual, graphical, relational, and numerical data in a number of ways, depending upon the data type and the informational needs of the user. Particularly important will be the future need to develop standardized approaches for rendering multimedia and virtual reality (VR) representations in models and simulations (e.g., using Virtual Reality Modeling Language). Such multimedia and VR capabilities are already being developed and evaluated in the U.S. Fire Administration. From an enterprise-wide architectural component perspective, this class of tools will, to the extent practicable, be transparent to the user and be invoked under systems control when needed. Composition capabilities will need to be provided for output to paper and electronic formats including future XML-based Web pages for information dissemination purposes, as appropriate.

- **Configuration Management Tools.** An important class of tools in the *FEMA IT Architecture* will be responsible for maintaining control over configuration item components within FEMA IT systems and networks. As standards for data formats change, technology evolves, and IT and network systems evolve, the need for a disciplined and standardized approach for configuration management increases. Enterprise-wide CM tools will allow controlled management of user data sets, system software, hardware, and related architectural components over time. The Technical Reference Model (TRM) and Appendix N list enterprise-wide configuration management tools that have been adopted.

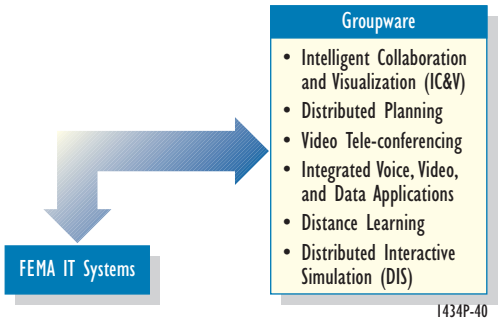
- **Systems Engineering Tools.** In order to develop and integrate robust and reliable architectural components for the *FEMA IT Architecture*, a set of powerful systems engineering and development tools is required. Computer-Aided Software Engineering (CASE) tools are intended to be a standardized architectural component. CASE tools will allow FEMA developers to develop accurate data and processing models for components of the IT infrastructure. Access to building blocks such as standardized data dictionary services, interfaces, and standard hardware/software/network components will ensure a high level of systems interoperability between the various components of the evolving *FEMA IT Architecture.*

- **Automated Software Update Tools.** As the components of the *FEMA IT Architecture* mature, and the underlying software components change, a mechanism will be required to ensure that system users are kept current in terms of software technology. A key component of the *FEMA IT Architecture* will be the automated software update function. This process will operate in the background and monitor user software configurations automatically. It will then provide updates and changes without user intervention. This process will help mitigate the complexities of change management in a distributed environment. See Appendix N for a list of automated software update tools.

- **Help Desk and 800-Number Services.** As the *FEMA IT Architecture* is implemented, new systems such as NEMIS come on-line, and future capabilities are designed and integrated, user support will be a critical component of the *FEMA IT Architecture.* User support will be provided in a number of ways, depending upon the technical area. Extensive use of on-line support and help systems will be provided to solve most common problems. Existing methods of providing hotline support within FEMA will be consolidated and harmonized. The architecture also envisions some consolidation and re-use of the number of 800-number lines. A hotline to an IT support desk will allow users to contact IT professionals when problems occur that cannot be readily solved by other methods.

1.12.6.11 Groupware

In the *FEMA IT Architecture*, groupware includes a class of tools that support distributed operations and business functions requiring persons to interact with each other on documents and data sets. In general, groupware tools need to be integrated across the enterprise to gain seamless access to digital library services, integrated systems and



services, enterprise-wide tools such as text search and rendering and display tools, and electronic mailroom services. In particular, an emerging technology trend for groupware is to utilize Java-based Web interfaces and Secure Socket Layer (SSL) services tools for collaboration.

In the structured discussions, groupware was a widely cited architectural need and requirement. Groupware can support operations and business functions such as (1) response and recovery where FEMA enterprise decision-makers are mutually sharing a digital map and comparing notes on objects that are geo-referenced on the map; (2) human services where an application has been filed and must be reviewed by a number of individuals who are distributed; (3) mitigation activity in sharing results of studies and analyses with distributed partners, the States, and Regions; and (4) training and exercise events involving distributed planning, reconstruction, analysis, and results dissemination.

The following briefly identifies the classes of tools and technologies that may be considered as groupware architectural components:

- **Intelligent Collaboration and Visualization (IC&V) Tools.** IC&V tools are considered an essential element of distributed digital library services. As the name implies, they facilitate collaboration and visualization of objects across the enterprise in an intelligent fashion. Through careful systems development and integration, IC&V tools are able to access and use other systems and services such as the RDBMS, workflow processes, text search tools, and rendering tools (to name a few). What makes these tools intelligent is their rich and value-added ability to exploit advanced distributed digital library services in ways that are intuitive and user-friendly. IC&V tools typically support voice, video, and data applications, though these data streams may not be integrated into a single data stream such as an ATM protocol could support.

- **Distributed Planning Tools.** Distributed planning tools are a class of groupware that supports planning functions where an optimum plan or course of direction is desired. Generally speaking, these tools tend to drive the distributed planning team toward a particular solution where all of the major variables have been explored and evaluated. Distributed planning tools typically have a modeling and simulation component to support the evaluation. They typically also have an optimization component. When combined with a GIS, distributed planning tools represent a powerful technology for developing and evaluating potential courses of action in advance of having to commit to a real world operation.

- **Video Tele-Conferencing (VTC).** FEMA currently conducts video tele-conferencing over its backbone network. This VTC currently transmits voice and video. The current VTC does not directly integrate a data stream or data source. Also, the Quality of Service (QoS) is not adaptive. VTC will continue to be a part of the target *FEMA IT Architecture*.

- **Integrated Voice, Video, and Data Applications.** Integrated voice, video, and data applications were frequently mentioned in the structured interviews. In the target *FEMA IT Architecture*, these integrated applications provide intelligent collaboration and visualization services (IC&V) as above. The major difference is that integrated voice, video, and data applications are carried on a single data protocol (such as ATM). The data protocol provides adaptive QoS and some measures of security. Integrated voice, video, and data applications are currently the subject of considerable R&D in projects such as the Next Generation Internet (NGI) and Internet2.

They also tend to be computationally and bandwidth intensive especially as they are integrated with very large distributed digital libraries containing large and complex objects. Interactive GIS is an example of a FEMA system that could benefit from such technology. As integrated voice, video, and data applications are developed, as the FEMA network evolves, and as the business case warrants, FEMA will consider incorporating such advanced applications into the *FEMA IT Architecture*.

- **Distance Learning.** Distance learning was a widely cited technology in the structured discussions. Strong proponents included Mitigation, PT&E, R&R, Emergency Management Institute, and the National Fire Academy. As a groupware concept, distance learning technology is a form of intelligent collaboration and visualization that supports interactions between the instructor and students in a distributed environment. Distance learning exploits and uses digital library methods and allows for multimedia. Depending on the number of students and simultaneous users, as well as the size of the objects that are being interchanged, distance learning can be very bandwidth intensive. This technology also places a premium on the network to provide multicast capabilities and bandwidth management. Within the *FEMA IT Architecture*, the major value of distance learning is that it affords an opportunity to reach a potentially large number of distributed individuals without the hassle of travel and face-to-face meetings. Distance learning has some potential for achieving cost savings, which needs to be further analyzed.

  Currently within FEMA, distance learning is being afforded via the Emergency Education Network (EENET). EENET is a satellite-based distance learning system to bring interactive training programs into virtually any community nationwide. This system provides fire and emergency management training on a regularly scheduled basis through EENET's *National Alert* monthly broadcasts, as well as a variety of special videoconferences, training courses, and town hall meetings. Schedules are updated periodically. All programming is open and is in the public domain. Any community with access to a C-band or Ku-band satellite dish, or a community cablevision provider, can receive the broadcast and participate in the training programs. In the target *FEMA IT Architecture*, EENET will continue to be used and exploited. Consistent with business case analysis, additional efforts will broaden the base of interactive distance learning using the Internet, the FEMA Intranet, and Extranets.

- **Distributed Interactive Simulation (DIS).** DIS is a protocol developed by the DOD to support widely-distributed exercises and training events. It is in routine use in conducting realistic training across all Services (e.g., Army, Navy, and Air Force). Individuals in the PT&E and Mitigation Directorates expressed an interest in evaluating this type of technology to potentially support FEMA training exercises and events. DIS is a distributed object-oriented and model-based approach that interchanges messages among exercise participants. With DIS, there is a requirement for exercise participants to share common data models, for example, a GIS-based map that provides *ground truth*. At each participating site, IT systems must also run models to keep the scenario going. DIS basically provides the data transport protocol to share events and decisions that are reflected in updates to individual site's data bases and displays. For DOD, DIS has been demonstrated to be an effective method of providing realistic distributed training in an exercise environment. DIS concepts need further evaluation in the FEMA environment. In particular, the potential impact on FEMA networks and IT systems providing digital library services needs to be carefully assessed.

2. TECHNICAL REFERENCE MODEL AND STANDARDS PROFILES

2.1 FOREWORD

2.1.1 Introduction

The Technical Reference Model (TRM) and standards profiles (both technical and security) make up a vital crosscutting element for FEMA IT systems, affecting virtually all components of the FEMA Enterprise Architecture. Increased use of open systems standards will enable interoperability, portability, and scalability in IT systems across FEMA. Standards must be consistent and uniformly applied throughout the Agency and across the enterprise. Standards form the basis for development of re-usable components of the FEMA Enterprise Architecture, and the Chief Information Officer (CIO) and Information Resources Board (IRB) will use established standards to guide and constrain IT asset acquisitions in the future. There are a number of technical, operational, and managerial issues associated with the application of standards for the creation, management, and use of electronic documents and data across the enterprise.

2.1.2 Background of the Technical Reference Manual and Standards Profiles

This updated *FEMA IT Architecture, Version 2.0,* provides the validated TRM and set of standards profiles developed by FEMA. The first TRM for FEMA was developed for the initial *FEMA IT Architecture, Version 1.0.* As noted in Section 1, the FEMA Information Technology Services (ITS) Directorate has indicated that an internationally-accepted, open systems, disciplined, and standards-based IT architecture will best meet FEMA's needs for designing and developing future information systems, for re-engineering legacy systems, and for achieving future integration and interoperability among systems across the broad and distributed FEMA enterprise. This TRM represents an important opportunity for FEMA to increase interoperability, redundancy, portability, and security across FEMA IT systems and to do so in an open systems fashion. A standards based TRM also simplifies user training and support.

Heretofore, the common practice of defining a standard at FEMA has been largely a matter of declaring that all organizational entities use the same standard tool, such as cc:Mail or Microsoft Word or PowerPoint. This approach clearly has its pros and cons. At one level, it is very expedient to declare a tool to be a standard and *pretty much* ensures that FEMA organizational elements will be able to instantly interchange and use data files among each other via electronic means. Despite the good intentions of national and international open systems standards organizations, FEMA observes that, unless there is a critical mass of vendor support for an open systems standard and a uniform method of implementing the standard (e.g., a widely-accepted Application Portability Profile [APP]), competitive proprietary approaches will tend to win out in the marketplace.

FEMA does not have the resources to develop its own suite of tools to implement open systems-compliant tools in lieu of appreciable vendor and industry interest and support. Furthermore, FEMA does not have the resources to develop standards profiles for use across the emergency management community. To achieve interoperability, FEMA strongly prefers to be a consumer or user of existing profiles.

On the other hand, the approach of declaring a tool, system, or application as the FEMA standard has tended to lock FEMA and other Federal agencies that have also done so into using certain vendors and their proprietary file formats. The major concerns with this approach are:

- Achieving interoperability with FEMA's external business partners, who may be using a different tool, is problematic. Achieving cross-agency and FEMA business partner consensus on tools continues to be a very difficult proposition.

- FEMA, like other Federal agencies, has virtually no control or influence over the tool vendor and the file format definition. There is always the concern that the file format might become an unsupported orphan and make it difficult for FEMA to migrate the data to a new tool without risking loss of data and document integrity.

- The tool vendor may go out of business or be sold to a competitor and the file format become an orphan or be completely re-engineered to not be reverse compatible.

- FEMA has little or no control over the standard tool releases or versions. Even if FEMA partners are using the same standard tool, they may be using different versions, and the data interchange may fail at that level.

- Lastly, the file and data formats for many industry standard and proprietary formats are not supported for long-term archival storage and retrieval purposes. Additionally, any translation to an acceptable archival format risks loss of document and data integrity. This situation is a common problem for other Federal agencies.

Notwithstanding the above, FEMA supports the implementation of open systems standards as a basis for achieving interoperability, transportability, and long-term data integrity. FEMA also notes that otherwise worthy open systems standards will languish if they do not receive a critical mass of support and interoperability testing from vendors. Similarly, vendors will only develop tools if they perceive a customer base and demand for the product. Thus, specifying an open systems standard helps to "make it be known" that FEMA and other agencies are ready customers and supporters of open systems.

In implementing open systems standards, FEMA desires the widest possible ability to interchange information. This implies that the standards and the supporting tools be tested and viable in large-scale, enterprise-wide operations. If only one vendor implements the standard, the information still may not be interchangeable across systems, especially if the vendor later drops the product. Even if two vendors implement the open systems standard just as Microsoft and Netscape have done by interpreting the requirements for Hypertext Markup Language (HTML) slightly differently in their Web browsers, there is still no guarantee of interoperability. Figure 2-1 illustrates the target concept for developing and implementing open systems.

As a practical matter for this TRM, FEMA will place appropriate emphasis on adopting open systems approaches but also recognizes the operational need to specify the use of a particular standard tool if no fully open systems approach is viable and tested.

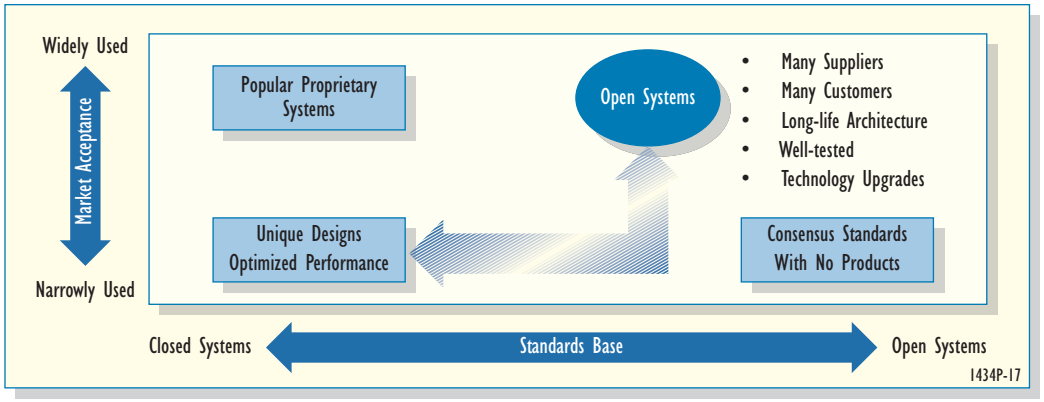


Figure 2-1. FEMA Target Concept for Implementing Open Systems Standards

2.1.3 Terms and Definitions

This section provides working terms and definitions for the following:

- **Technical Reference Model (TRM).** A TRM is a model that provides the basic ground rules, set of standards, or building code for designing, developing, implementing, testing, and integrating IT systems. The TRM identifies and describes the basic information services (such as data base services, document management services, security services, etc.) at a high level, and how they ought to be designed and constructed in a uniform and standardized manner.

- **Standards Profile.** A standards profile defines how a particular standard such as an open systems standard, an industry standard, or a standard tool needs to be customized or tailored to support interchange or interoperability. A profile recognizes that all major standards generally need to be customized or profiled through establishment of user conventions. These profiles or user conventions are frequently referred to as Application Portability Profiles (APPs).

- **Standard Tool.** A standard tool is defined as an IT tool, system, or application that FEMA has determined to meet operational requirements and is mandated for use in IT systems. A standard tool is part of the *FEMA IT Architecture*.

- **Security Services Model.** A security services model is the TRM for security services (such as access controls, confidentiality, fault tolerance, originator authentication, etc.).

- **Security Standards Profile.** A security standards profile is the same as a standards profile except that it refers to security standards.

2.1.4 Goals and Objectives

Table 2-1 identifies the goals and objectives of the FEMA TRM and standards profiles.

Table 2-1. Goals and Objectives

Goals and Objectives	Description of Development Opportunity
Interoperability	Promotes interoperability through defining the basic building code or building blocks for systems and makes the requirements be known to FEMA's enterprise partners, developers, and integrators.
Stability	Provides a stable base for development of IT systems.
Re-use	Promotes re-use through establishment of standardized architectural components that are mandated for use in new developments and re-engineered or re-hosted systems.
Portability	Promotes portability through emphasis on selecting open systems approaches wherever practicable.
Longevity of Data	Helps ensure longevity of data by formally defining and/or profiling a standard. If a vendor or a standard tool goes out of business or is withdrawn, the definition and profile of the standard can be used to recover and/or read the legacy data.
Cost Effectiveness	Promotes cost effectiveness through establishment of common approaches for re-use.
Compatibility with National Institute of Standards and Technology (NIST) TRM	To promote interoperability across Federal agencies, the FEMA TRM is compatible to the maximum extent practicable with the NIST TRM.
Year 2000 Compliance	Firmly establishes the architectural baseline and ground rules for achieving Year 2000 compliance. All FEMA architectural components shall be Year 2000 compliant.

2.1.5 CIO Directives for Application of the Technical Reference Model and Standards Profiles in FEMA IT Systems

To achieve the goals of interoperability and consensus across the emergency management community, FEMA will use and exploit existing standards and proven standards profiles, wherever practicable. The following directives and guidelines shall apply:

- FEMA is committed to employment of open systems standards wherever practicable to achieve the goals and objectives identified above. An open systems life-cycle approach that is workable and viable is strongly preferred over proprietary approaches, which might be more expedient.

- The TRM and standards profiles shall be applied to the development of both enterprise-wide IT systems and standalone, program-centric systems to the maximum extent practicable.

- The *FEMA IT Architecture* (including the TRM and standards profiles) is considered a living document. Updates and revisions will be made as required. The *FEMA IT Architecture* document shall be under strict configuration management and control.

- Consistent with the architectural principles in Appendix H, any FEMA organizational element or established business partner may request waivers, deviations, or exceptions to the *FEMA IT*

Architecture. They may also propose modifications, additions, clarifications, and updates to the *FEMA IT Architecture* (including TRM and standards profiles). Section 4 of the *FEMA IT Architecture* provides guidelines for requests of waivers, deviations, and exceptions.

- The TRM and standards profiles shall apply across the life cycle of an IT system.
- The TRM and standards profiles shall be used in major IT systems acquisitions and developments. It is recommended that a technical approach for achieving compliance be part of the evaluation factors.
- The CIO seeks to apply IT standards and standard tools consistently and uniformly throughout the organization.

2.2 FEMA TECHNICAL REFERENCE MODEL

2.2.1 Key Architectural Issues Associated with Standards

There are a number of important technical and managerial issues that impact multiple Federal agencies and are currently beyond the control of FEMA. Some of these architectural issues are still unsettled across the IT community and with the National Archives. In general, these issues are contributing to the difficulty that Federal agencies like FEMA have in implementing open, interoperable, and standardized approaches in consensus with their business partners. These unsettled issues contribute, as background factors, to FEMA's status as a consumer, not a developer, of standards and standards profiles. Eight of these issues are stated and discussed in Appendix K.

2.2.2 Identification and Description of Major FEMA IT Services

The major IT services and architectural components are identified and described in Appendix N. Appendix H also identifies the relevant IT standards or standard tools and their status at FEMA and provides appropriate comments.

Standards for networking services and communications services are separately addressed in Section 3. The requirement for security architecture and security standards is addressed in Section 2.4. Minimum requirements for the FEMA standard workstation (e.g., processor, memory, video display, data storage and input/output (I/O) media, network ports, energy conservation, monitor, etc.) are stated in the *FEMA Information Resources Management Procedural Directive (FIRMPD)*.

2.3 FEMA STANDARDS PROFILES

2.3.1 Nature of a Standards Profile

Because of its relatively small role in the marketplace and in light of the crosscutting issues referred to in Section 2.2.1 and discussed in Appendix K, the FEMA CIO will not develop standards profiles. FEMA may adopt, very selectively, and exploit existing and widely accepted standards profiles in close coordination with FEMA's business partners. As a general practice, FEMA will purchase and use the tools that the Agency finds to offer the best overall advantage.

2.3.2 Identification of Major IT Standards in the FEMA High-Level Technical Reference Model Framework

Selected standards that offer significant potential for achieving openness across FEMA's IT systems in the future are identified in Appendix O.

2.4 FEMA SECURITY ARCHITECTURE

With this updated *FEMA IT Architecture*, *Version 2.0*, the need for a FEMA Security Architecture framework has been established. FEMA clearly recognizes the critical importance of a detailed Security Architecture and is currently in the process of implementation. A robust, fully implementable, and comprehensive FEMA Security Architecture is recognized to be important for future IT systems development and integration at FEMA.

The purpose of this section of the FEMA TRM is to provide the high-level guidelines and to describe the preferred methodology for development and implementation of the FEMA enterprise-wide Security Architecture.

Accordingly, this section defines a standardized architectural approach for:

1. Identifying required security services for FEMA IT systems and networks

2. Analyzing the security implications and requirements for IT systems and networks

3. Allocating security mechanisms to meet the requirements.

This section of the TRM also provides high-level security architecture guidelines for FEMA information system developers as they plan for the hardware and software design implementations. System developers need to determine if security measures that they are implementing in their systems provide sufficient services for authentication, access control, data confidentiality, data integrity, availability, and non-repudiation, or whether additional system-specific security services and mechanisms must be developed.

2.4.1 Methodology for Development of a Security Architecture

This FEMA TRM considers the basic concepts described in the following documents as a methodology for development of an enterprise-wide FEMA Security Architecture:

1. *Department of Defense Technical Architecture Framework for Information Management (TAFIM), Volume 6, Department of Defense Goal Security Architecture (DGSA)*

2. *International Standard, ISO 7498-2, Information Processing Systems—Open Systems Interconnection—Basic Reference Model, Part 2: Security Architecture.*

The two documents identified above provide proven high-level architecture development concepts that have been widely used throughout government and industry for the development of security architectures. The methodology is responsive to the requirements of PDD-63 to address and analyze the security of cyber systems and networks, as well as the NIST policies, standards, and guidance.

2.4.2 Goals of the FEMA Security Architecture

One of the major goals of the FEMA Security Architecture is to define where in the overall information systems architecture security services need to be provided. The FEMA Security Architecture will also define the mechanisms to provide the required services. As the *FEMA IT Architecture* is implemented, the FEMA Security Architecture will allow system developers to determine what, if any, enhancements must be made to development programs to meet the security requirements.

Since it is impossible to foresee all future security requirements, the FEMA Security Architecture must be flexible to meet the requirements of both today's FEMA information systems and near-term development programs. Future *FEMA IT Architecture* developments that might impact the security service allocations include widespread implementation of groupware based on emerging approaches such as Java, or establishment of Virtual Private Networks (VPNs) with FEMA business partners.

2.4.3 Security Architecture Development Approach

As noted above, the Department of Defense (DOD) Goal Security Architecture (DGSA) document and International Standards Organization (ISO) 7498-2, Part 2, *Security Architecture* document provide a recognized methodology for developing a FEMA Security Architecture. Critical to any security architecture development are the required security services and the assigned or allocated security mechanisms. Each of these is briefly addressed.

2.4.3.1 Security Services

Within the FEMA Security Architecture, security services are the basic functions that must be provided. These fall into six internationally-agreed upon areas. At the current level of development of the *FEMA IT Architecture*, the FEMA Security Architecture needs to consider the following basic security services:

- **Authentication.** These services establish the validity of a claimed identity.

- **Access Control.** These services prevent the unauthorized use of a resource, including preventing the use of a resource in an unauthorized manner.

- **Data Confidentiality.** These services protect data from unauthorized disclosure.

- **Data Integrity.** These services protect the integrity of data and detect any modification, insertion, deletion, or replay of any data within the system.

- **Availability.** This service ensures resources, applications, and data can be accessed by users for a predetermined percentage of the time.

- **Non-repudiation.** These services provide either proof of origin of data or proof of delivery of data or both. They protect against any attempt by either the sender or the receiver of the data to falsely deny sending or receiving the data.

- **Audit Services.** In addition to the six security services, audit services are added to the FEMA Security Architecture. Included with the audit services are intrusion detection and audit reduction mechanisms. Audit services are considered a part of security management in the ISO standards.

2.4.3.2 Security Mechanisms

Security mechanisms are defined as administrative measures, physical controls, and hardware and software functions that can be configured and allocated to satisfy the required security services. In the interest of open systems development, FEMA anticipates that the FEMA Security Architecture will define the functions that will be provided, and not necessarily the actual hardware and software. For example, the FEMA Security Architecture may call for a distributed directory structure without specifying which directory system (UNIX, Windows NT, etc.) will be used. These functions can be thought of as the actual high-level engineering design solutions to provide the required services. This *FEMA IT Architecture* anticipates that in many instances more than one mechanism could be used to provide a required security service.

2.4.4 Security Architecture Methodology

As noted above, both the DGSA and ISO 7498-2 will be considered in the implementation of the FEMA Security Architecture. ISO 7498-2 primarily establishes the service definitions. The DGSA provides a good high-level methodology for development of security architectures. Consistent with the DGSA approach, Figure 2-2 provides the high-level framework that will be used for developing and characterizing the FEMA Security Architecture.

As illustrated above, the major FEMA Security Architecture elements to be considered include:

- **Local Subscriber Environment (LSE).** The LSE will include the devices and communications systems under user control. An LSE may contain a single end-user system such as a workstation, a single relay system such as a router, or a complex interconnection of end systems and relay

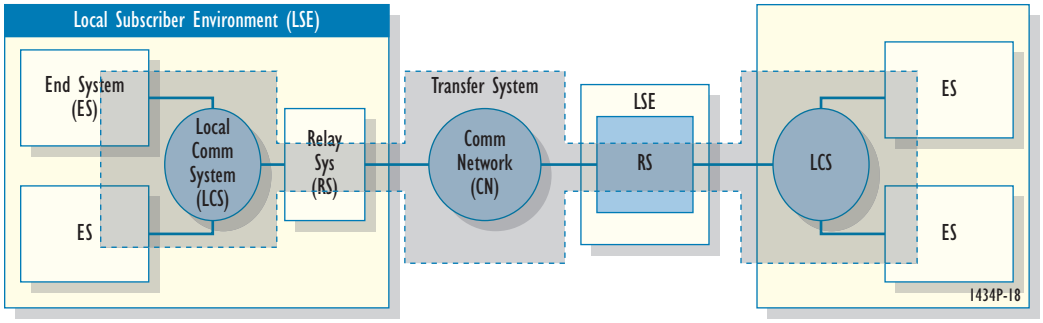


Figure 2-2. Generic Systems and Network Representation Approach to Develop the FEMA Security Architecture

systems connected through local communications systems. Prime examples of LSEs are computer rooms (such as FEMA command centers, Disaster Field Offices, and end-user office environments).

- **End System (ES).** ESs consist of a single element, such as a workstation, server, or mainframe. These systems are the basic building blocks of the architecture that provide the data storage and data processing functions.

- **Local Communications System (LCS).** The LCS consists of the networks within an LSE that supports connection of end systems and provides the interface to relay systems. These are the local area networks (LANs).

- **Relay System (RS).** The RS consists of communications devices such as multiplexers, routers, switches, cellular nodes, network firewalls, and message transfer agents. The RSs usually provide the interfaces to LSEs and CNs within the *FEMA IT Architecture*.

- **Communications Network (CN).** The CN defines the communications connecting the LSEs and may be a communications network entirely under control of FEMA, such as the FEMA Switched Network or may be a public communications entity such as the Internet or other leased networks.

- **Transfer Systems (TS).** TSs can be viewed as the end-to-end application subsystems that make up FEMA's information systems. The TS might typically be composed of a NEMIS user workstation, the FEMA Switched Network (FSN) backbone, a server or mainframe located in FEMA Headquarters, and applications that reside on the individual end systems.

2.4.5 Information Assurance Program

FEMA is responsible for protecting its own critical infrastructure, especially its cyber-based systems. The critical infrastructure includes the physical and cyber-based systems essential to the operations of economy and government. FEMA also recognizes that close cooperation with State and local governments and first responders is essential for a robust and flexible infrastructure protection program. The CIO for FEMA also serves as the Agency's Chief Infrastructure Assurance Officer (CIAO).

FEMA has developed a comprehensive Information Assurance Program which complies with Executive Order (EO) 13010, Presidential Decision Directive 63 (PDD-63), Office of Management and Budget (OMB) A-130, the *Government Information Security Reform Act* (enacted in October 2000 as part of the 2001 *Defense Authorization Act*) and the security policies, standards, and guidance issued by NIST.

FEMA is consequently well protected from outside attack and is improving protection from inside threats. FEMA is proceeding to build an enterprise-wide security program. The complete Information Assurance Program is discussed in detail in the following section.

2.4.5.1 Actions Completed

Protections Implemented
FEMA has established a strong perimeter defense, established an Incident Response Team, established strong virus protection, including all PCs and e-mail scanning, and prepared and implemented protection for www.fema.gov.

Configuration Control Established
An agency-wide Configuration Management Program has been established. Standard Web site Service Configurations have been established and controlled. Configuration of the Intranet is strictly controlled. Automatic configuration verification scans are performed on the network switches and routers every night to verify configuration has not changed.

Vulnerability Assessments
Nine (of 13) Critical System Assessments were completed in November 2000. Security plans for nine systems have been completed. Evaluation of the perimeter and Intranet found a well-designed security architecture and policies.

Prohibited Activities Identified/Employees Notified
Warning banners have been placed on all National Emergency Management Information System (NEMIS) servers and routers. Modems in machines connected to the network are prohibited. Modem scans are run regularly on FEMA phone lines.

Outcomes to Date
There has been no successful hacking attempt. There has been only minor impact from serious virus attacks. Only one very minor Web page alternation has occurred in over six years of on-line presence.

2.4.5.2 Next Steps

Enterprise Security Plan
An enterprise-wide Security Plan will be developed from the integration of the 13 critical systems plans, Agency policy, and the external requirements of PDD 63, the *Government Information Security Reform Act*, and NIST guidance. The schedule includes:

- Implementation of the CIAO Critical Infrastructure Protection (CIP) identification guidance in February 2001
- Update of the Security Section of the FIRMPD in July 2001
- Update of the Enterprise Security Response Manual in July 2001
- Incorporation of OMB A-130 and NIST guidance in the draft Enterprise Security Guide in November 2001.

Vulnerability and Risk Assessments and Accreditation Process
Assessments and Security Plans for the remaining four systems will be completed during FY 2001. Risk assessments for all 13 systems are due to be completed by fall 2001. The Accreditation Process has been developed.

Human Factor
FEMA will improve information assurance training, awareness, and accountability; implement an enhanced training and awareness program; tighten up the employee exit process; and increase the visibility of system monitoring.

Training and Awareness Plans
Standard Security Awareness Briefings will be provided to new hires. An Enterprise Security Web page will be developed. Security awareness e-mail tips will be provided to all FEMA employees. A Web-based Security Administrators Program will be implemented. A Web-based User Awareness Program will be developed.

Accountability Plan
The new hire processing formally warns employees of their responsibilities, prohibited practices, and penalties for improper activity. The system password process is being modified to enforce the current password size and duration policy. Actions are being taken to increase employee awareness of the monitoring of critical systems users.

Enhance Intrusion Detection and Response
FEMA will establish a 24/7 Intranet and perimeter monitoring for intrusion attempts during FY 2001 and add additional Incident Response Teams.

Establish Security Monitoring Program
FEMA will establish a certification process and certify all FEMA systems in risk assessments, security plans, and system accreditation. FEMA will monitor Information Assurance Program activities including security and contingency testing, personnel programs, and compliance with identified remedial actions including audits.

This page intentionally left blank

3. COMMUNICATIONS AND NETWORKING

3.1 OVERVIEW

This section emphasizes the network architecture. To provide a point of reference, the existing FEMA network configuration is described at a high level. More detailed configuration information for the current network can be obtained from the FEMA National Network Operations Branch (NNOB).

The *FEMA IT Architecture, Version 1.0*, identified major near-term recommendations including the following:

- High-performance, high-availability switched backbone
- Increased network efficiency through modern compression and bandwidth sharing
- Integrated voice, video, and data communication services
- Leveraged use of public switched services and VPNs

The first three recommendations have been largely implemented. High speed Asynchronous Transfer Mode (ATM) switches are deployed at major FEMA locations across the country. The switches provide carrier class survivability and near-instantaneous rerouting capabilities. The switches also provide the ability to dynamically allocate bandwidth with the required level of Quality of Service (QoS). The QoS features have enabled voice services to be integrated into the common backbone network. Advanced voice compression techniques are used to achieve an eight-to-one improvement in bandwidth utilization. In addition to voice integration, new video systems and gateways are being deployed to achieve greater efficiencies and more capabilities so that legacy dedicated circuits can be phased out.

The new integrated network has substantially improved performance, reduced congestion, and increased efficiency. Most importantly, the network integration project has positioned FEMA to rapidly expand services in the event of a major disaster.

The rapid growth in computers, applications, and communications technology require a flexible and scalable growth strategy for the foreseeable future. This is being achieved through implementation of the IT architecture and the network architecture. FEMA is well positioned to manage growth through use of a switched backbone, QoS, and integration of voice, video, and data services. FEMA is also ready to take advantage of public switched services, which can provide significant bandwidth scalability without the burden, or expense, of maintaining the network. Other important network services are under consideration in the target network architecture. The implementation strategy describes a phased approach that includes prototypes, legacy support, and an event-driven milestone schedule.

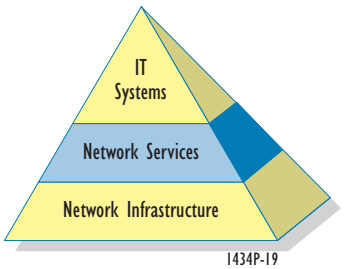


Figure 3-1. Network Architecture Model

3.1.1 Network Architecture Components

As shown in Figure 3-1, the FEMA network architecture model consists of three major layers or components: network

infrastructure, network services, and IT systems. The network infrastructure is the foundation for the higher layers. The network services component provides a variety of services and supports IT systems and other user elements.

3.1.2 Network Infrastructure

The network infrastructure consists of several elements: transmission, switching systems, and network equipment. Of these, transmission is a significant recurring cost driver. Transmission is composed of backbone connections (mostly wide-area) and access tail-circuits (mostly local-area). Satellite transmission and reception facilities are also important parts of this component.

Switching systems consist of voice switches (PBX), data switches, routers, digital cross-connect switches, and multiplexers. These elements appear in both the wide-area and local-area portions of the network.

3.1.3 Network Services

Network services include voice, video, data, and help desk services. Network services also include important internal functions such as network management and security. Network services may also include services such as virtual private networks (VPNs) and multimedia services (in the future).

3.1.4 IT Systems

IT systems include user elements and enterprise systems such as the National Emergency Management Information System (NEMIS). IT systems also include support of unique Regional and field requirements and systems such as servers, virtual local area networks (LANs), and network addressing. Other potential services include Personal Communications Services (PCS), mobile services, bandwidth on-demand, Quality of Service (QoS), and security. In addition, the network may need to support enterprise-wide IT services such as (in the future) correspondence and action tracking, text search, digital signature, collaboration and visualization services, interactive geographic information system (GIS), and digital library services. Several of the IT services discussed above now appear as specific projects in FEMA's Target Architecture Capabilities discussed in Volume 2, Appendix P.

3.1.5 Network Architecture Process

In developing the FEMA network architecture, the Information Technology Services (ITS) Directorate reviewed existing documentation, evaluated vendor products, and interviewed key personnel. This effort included the following major activities:

- Understand FEMA mission and networking requirements, and define baseline:
  - — Study network documentation and diagrams
  - — Interview key operations and engineering personnel, and tour facilities and equipment.

- Assess network infrastructure for each type of service:
  - — Circuit and node utilization analysis

— Network management, problem detection, and diagnosis
— Deficiencies, points of failure
— Maintenance emphasis and issues
— Growth patterns and projections.

- Identify alternatives, enhancements, upgrades, and new technology:
  — Vendor product evaluations
  — Integration of voice, video, data, and network management
  — Support of *FEMA IT Architecture* recommendations (new functions and technologies).

- Recommend evolutionary approach:
  — Proof-of-concept demonstrations
  — No downtime, phased integration, hybrid approach
  — Transition milestones based on needs and events:
    • Capacity, cost/benefit
    • Performance, availability
    • Training and readiness.

3.2 EXISTING NETWORK ARCHITECTURE

This section provides a high-level overview of the existing FEMA network architecture. The primary purpose is to provide a baseline and context for the discussion of architecture requirements and alternatives presented in later sections.

The existing network architecture is a snapshot taken during the initial *FEMA IT Architecture* and Network Technology Architecture (NTA) development process. It was validated with the updated *FEMA IT Architecture, Version 2.0*. As shown in Figure 3-2, the NNOB is a part of the Operations Division and maintains current configuration information for FEMA communications networks.

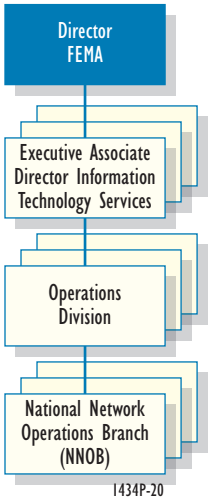


Figure 3-2. National Network Operations Branch (NNOB)

The following sections describe the existing network architecture in three major subsections: Network Infrastructure, Network Services, and IT Systems and User Elements.

3.2.1 Network Infrastructure

FEMA has two primary networks: a switched network and a data network. An overlapping network of point-to-point and switched connections provides the transmission infrastructure for both networks.

Within FEMA, the term *FEMA Switched Network (FSN)* generally refers to the entire enterprise of voice, data, and supporting networks. Figure 3-3 illustrates the enterprise network, which is divided into Regions, States, and other territories.

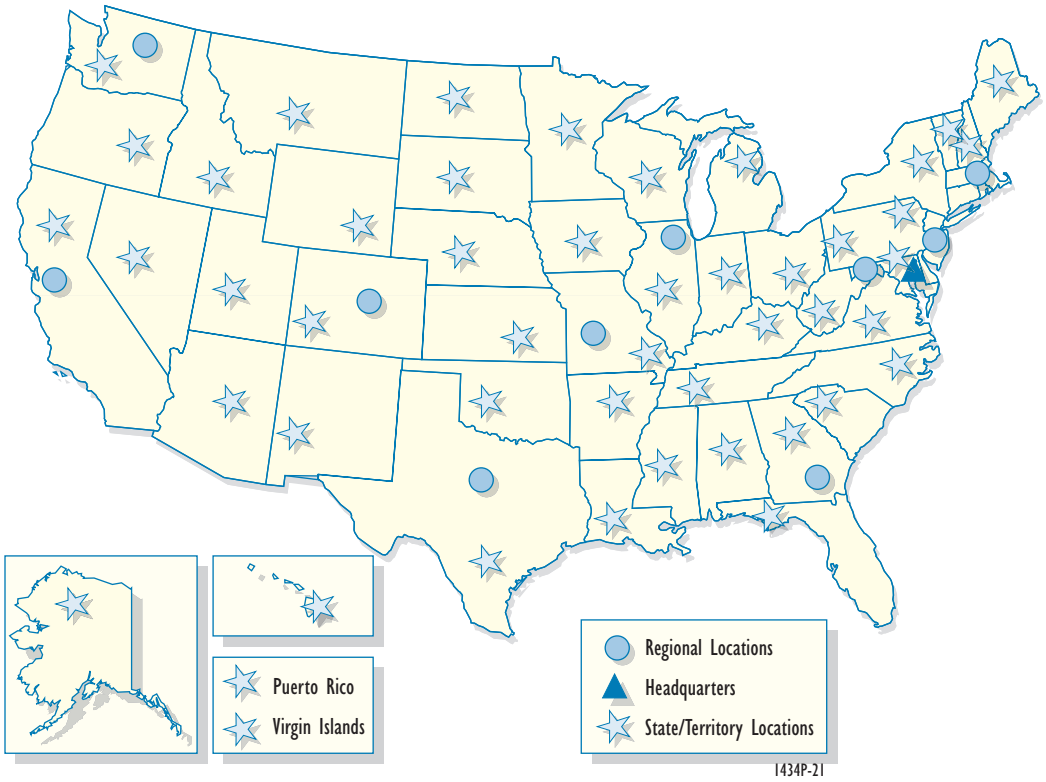


Figure 3-3. FEMA Enterprise Network

FEMA personnel also frequently use the term FSN in reference only to the voice network. For purposes of this document, the meaning of the term FSN will be more clearly stated. The terms *voice network* or *switched network* are used to refer to the Public Branch Exchange (PBX) network, which primarily provides voice services to FEMA. The term *data network* refers to the router network, which primarily provides data services.

3.2.1.1 Switched Network

The primary function of the switched network is to transport FEMA voice communications. A network of PBXs and multiplexers is used to provide a variety of voice and dial-up services. The switched network also provides external connections via the Public Switched Network (PSN) and the Federal Telecommunications System (FTS). In addition, the switched network can transport data and video connections via the integrated multiplexers. The PBX switching architecture is shown in Figure 3-4.

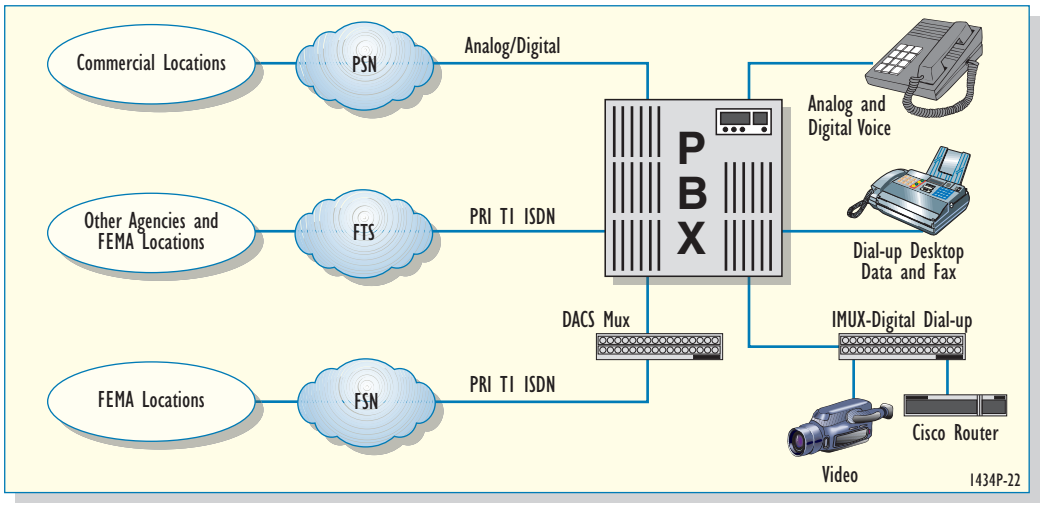


Figure 3-4. Switched Network Configuration

The primary nodes of the current switched network are interconnected in a hierarchical configuration. Mt. Weather, VA; Washington, DC (Headquarters); Hyattsville, MD; Atlanta, GA; Philadelphia, PA; Denver, CO; and Denton TX; are at the top of the hierarchy. Dedicated connections to the Disaster Field Offices (DFO) are provided from Mount Weather.

The PBX switches are programmed to route calls in the most cost-effective manner. The first priority is to route calls over the dedicated switched network (FSN). If the location is not reachable for any reason, the next path choice is FTS followed by the PSN. Figure 3-5 illustrates the connectivity of the primary nodes and locations in the switched network.

3.2.1.2 Data Network

The primary function of the current data network is to transport FEMA data traffic over the FEMA Intranet. The data network also has connections to the public Internet via firewalls. As shown in Figure 3-6, a network of routers is currently used to extend FEMA data services across the country and to other territories. The connectivity between routers is provided primarily by dedicated T1 circuits. Some connectivity is provided over the switched network using dial-up connections and multiplexers.

At each FEMA location, the routers provide connectivity for enterprise servers, LAN segments, and other clients. Switches and hubs distribute the connectivity to the LAN segments. The network contains approximately 80 routers and 94 Ethernet switches.

Three types of routing protocols are currently run on FEMA routers. Cisco's proprietary Interior Gateway Routing Protocol (IGRP) is used to route Internet Protocol (IP) traffic, Routing Information Protocol (RIP) is used to route Novell Internetwork Packet Exchange (IPX) traffic, and Enhanced Interior Gateway Routing Protocol (EIGRP) is currently running on a few FEMA

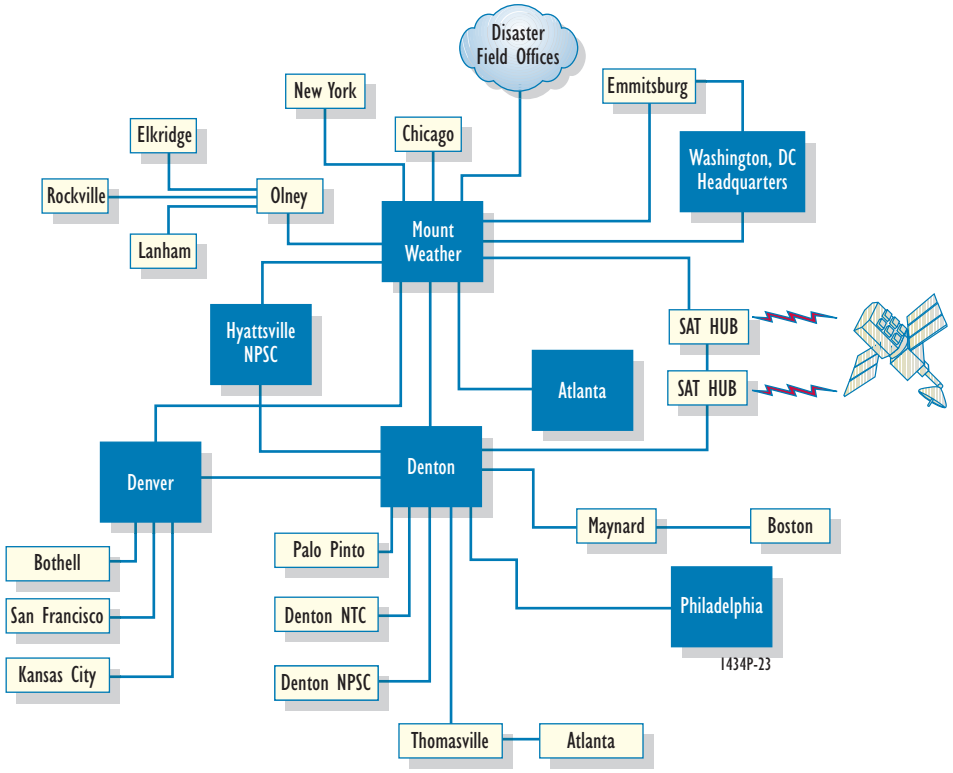


Figure 3-5. Switched Network Connectivity

routers. IP address segments are provided from a single class B address. In the future, FEMA may transition to a single consolidated routing protocol. The plan is to have EIGRP running on all FEMA routers by fall 2001.

High speed ATM switches are deployed at major FEMA locations across the country. The switches provide carrier class survivability and near-instantaneous rerouting capabilities. The switches also provide the ability to dynamically allocate bandwidth with the required level of QoS. ATM is further discussed in Section 3.4.3.4.

3.2.1.3 Transmission

In the current network architecture, the primary transmission medium is the Integrated Services Digital Network (ISDN) PRI T1. Both the switched network and the data network rely heavily on T1 transmission. Satellite transmission (T1) is used to quickly establish connectivity in disaster areas. The satellite connection is replaced by traditional T1 circuits when the local infrastructure can support it.

Due to the separate origins of the data network and the voice network, there are separate voice (switched) and data T1 circuits to most FEMA locations. Table 3-1 is a summary of the T1 circuits.

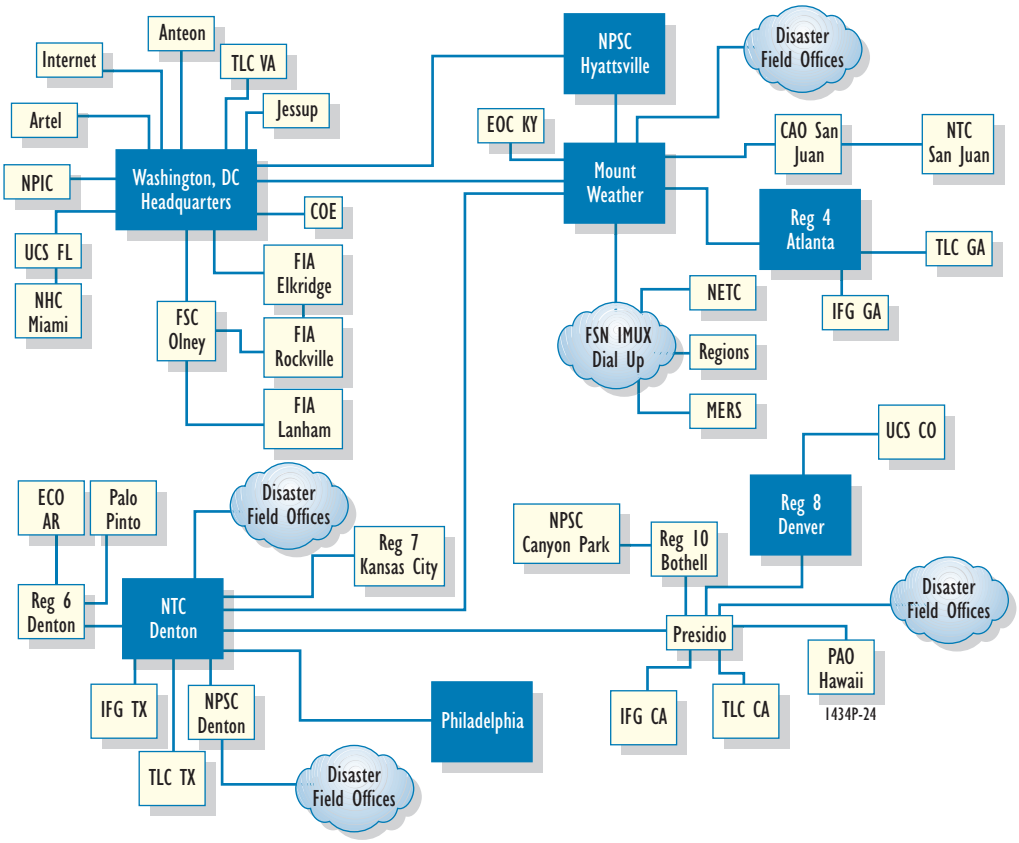


Figure 3-6. Data Network Connectivity

Table 3-1. T1 Summary

Network	Quantity of T1 Circuits
Data	47
Switched (Voice)	39
Total	**86**

3.2.1.4 Network Equipment

The National Network Operations Center (NNOC) at Mt. Weather currently maintains centralized control and management of network equipment. Table 3-2 summarizes the major types of network equipment. The quantity of equipment listed in the table is nominal and changes over time due to disaster support and routine maintenance. These quantities do not include the communications equipment in the Mobile Emergency Response System (MERS) and Mobile Air Transportable Telecommunications System (MATTS).

Table 3-2. Major Network Equipment Types

Network Equipment Type	Description
PBX	Private Branch Exchange switches. Quantities: 5 Merlin, 2 Meridian SL1, 9 System 85, 20 G3, and 2 G2
Multiplexers	Aggregate communications channels for transport over switched network. Quantities: 32 Inverse Multiplexers, 80 DACS and subrate multiplexers, and 15 IDNX multiplexers
Routers	Cisco routers for data network. Quantities: 90
Voice Messaging	Audix. Quantities: 11

3.2.2 Network Services

FEMA provides a number of network services including the following:

- Voice, video, and data
- E-mail and messaging
- Local and wide area connectivity
- Ordering and billing
- Cellular phones and pagers
- Point-to-point and dial-up circuits
- Facsimile
- Desktop services
- Security (physical and logical)
- Bandwidth management
- Network and systems management
- Configuration management
- Help desk and trouble reports.

Two of the services, *network and systems management tools* and *network security*, are discussed in more detail below.

3.2.2.1 Network and Systems Management Tools

Several network services and equipment require special tools and expertise. Table 3-3 lists standard tools currently used to provide network and systems management services.

3.2.2.2 Network Security

Network security is an important requirement for FEMA networks. Currently, FEMA data networks are protected with physical and logical security measures. The networks provide limited points of access and highly restrictive firewalls. All new products and technologies must be carefully evaluated for security risks. Network security will be addressed in more detail as part of the planned FEMA Security Architecture mentioned in Section 2.4 and in response to Presidential Decision Directive 63 (PDD-63) on Critical Infrastructure Protection (CIP).

Table 3-3. Standard Tools Used for Network and Systems Management

Service Category	Software Product Name	Description
Network Management	Hewlett-Packard OpenView	Provides platform for network management applications.
	Cisco Works for Switched Internets (CWSI)	Manages Cisco switching platforms. Cisco Works Detailed management of all Cisco routers.
	NetSys	Network debugging tools for managing, tuning, and planning growth of FEMA networks.
	Routing Control System (RCS)	System for changing configuration of 800 call routes.
	Call Management System (CMS)	Four locations to do agent traffic analysis.
	Comsphere 6800	Manages TDM multiplexers including 745 DACS Mux and 740 Channel Mux.
	ProCom	No Network Management system for IMUX. Use PC with ProCom to dial-up IMUX.
	NetOpen 5000	Manages IDNX.
	G3-MA	Manages G3 PBX.
	Monitor I	Traffic statistics and analysis (PBX).
Systems Management	System Programming and Maintenance (SPM)	Tool to configure Merlin. SPM software allows System Administrator to program system features and make moves and changes.
	Remedy Trouble Ticketing	Used by the NNOC to create and track network and system failures and errors. These are created by help desk support personnel or NNOC technicians.
	Voice Management System	Tool to manage PBX. At each site with PBX.
	Manager 4	Tool to administratively manage System 85 and G2.
	Accumaster Trouble Tracker	Used by the NNOC to create and track network and system failures and errors for the Lucent voice components.
	Accugraph	Provides physical configuration management.

3.2.3 IT Systems and User Elements

As mentioned in the previous section, several types of services are necessary to operate and maintain the network. At a higher level of the functional hierarchy, enterprise-wide information systems also need to be provided and supported. The most significant FEMA IT system currently being fielded is NEMIS. Other IT systems requiring care and attention in the existing networks are discussed in Sections 1 and 4 of this document.

3.3 REQUIREMENTS AND OPPORTUNITIES

The assessments and recommendations in this section are based on analysis of FEMA documentation and a series of discussions among FEMA engineering and operations personnel.

Overall, existing FEMA networks currently satisfy all mission-critical requirements. Sufficient bandwidth exists in both the voice network and the data network. Separate network management systems and tools and experienced staff provide FEMA with a responsive network management capability. With current systems, FEMA engineers and technicians can quickly install and troubleshoot network components in emergency situations and adverse environments.

While the current network architecture functions well, the performance and cost effectiveness of FEMA networks can be significantly improved. New network technologies can also expand and improve the current network services. The following paragraphs and later sections discuss potential requirements, opportunities, alternatives, and architecture recommendations.

3.3.1 Integration of Backbone Transmission

As previously described, FEMA effectively operates and maintains two distinct networks. Each network is essentially supported by separate transmission networks. There is some sharing of transmission via multiplexers and dial-up circuits, but the majority of transmission bandwidth is not shared. Significant savings in equipment and recurring costs can be realized if both types of network traffic can be shared over a single transmission network.

3.3.2 Voice Over Data Networks

FEMA has integrated voice over data networks. A voice over data network, such as IP, is a technology that potentially offers unique cost savings and new capabilities. Costs can be reduced by shifting some of the voice traffic to the data network where bandwidth is more effectively shared. Costs could also be reduced by reducing the amount of equipment required at some locations, particularly disaster areas.

Voice over data networks offer other advantages, particularly to disaster areas. For example, in deployments to disaster areas, separate T1 circuits are currently ordered for voice and data communications. Due to regulatory differences, the data circuits can be expedited and installed prior to the voice circuits. With voice over data networks, voice service could be established at the same time as the data service.

The integration of voice over data networks addresses QoS, gateways between the data and voice networks, and reliability. The QoS features have enabled voice services to be integrated into the common backbone network. A related capability that is under consideration as a potential network architectural component is Computer Telephony Integration (CTI). The value of integrating common desktop functions needs to be evaluated against the cost of implementation and support.

3.3.3 Integrated Network and Configuration Management

While current network management systems operate effectively, there is a significant opportunity to automate and simplify. As shown in Table 3-3, numerous systems and tools are currently required to manage and monitor the networks. In addition, an around-the-clock staff of cross-trained technicians is required to attend each system. Potential architectural improvements under consideration include provision of tools that would provide automated discovery of network configuration changes and correlation of alarms. The integrated presentation of network performance, problems, and configuration information is also being investigated.

3.3.4 Internet Protocol Address Management

Related to the issues of network management is the issue of IP address management. Current IP management is essentially a manual process. While this process works effectively today, there is generally a need to implement methods that can increase mobility, reconfiguration time, and manageability.

3.3.5 Derived *FEMA IT Architecture* Network Requirements

In developing the initial *FEMA IT Architecture, Version 1.0,* and the updated *FEMA IT Architecture, Version 2.0,* FEMA identified a number of potentially important operational factors that impact the target network architecture.

3.3.5.1 Multicasting

The broadcast or multicast of information to disaster areas and supporting organizations is an important capability that must be supported by the target network architecture. For example, within FEMA, the Office of Public Affairs currently broadcasts multimedia to disaster areas using a proprietary methodology. Due to network and application limitations, the number of simultaneous connections is limited to 60. However, in the event of a large disaster, it will be necessary to disseminate information to a much wider audience, on the order of tens of thousands or greater.

3.3.5.2 Extranets and Virtual Private Networks

IT architecture discussions with the FEMA Regions indicated a need for better networking to State and local governments and other Regional assets. Since FEMA security policies and firewalls restrict external access, a better method of communicating within Regions is required. The Regions specifically expressed a desire to evaluate and prototype Extranets and Virtual Private Networks (VPNs) to provide increased flexibility, bandwidth, and control within Regions. As stated previously, security issues need to be evaluated to ensure that the integrity of existing networks is not degraded. Similarly, network management systems and policies may need to be enhanced (or decentralized) to maintain smooth operations and support. These requirements are now under consideration for potential impact on the network architecture.

3.3.5.3 High Bandwidth

The projected need for more bandwidth is a commonly stated requirement among FEMA organizations. As an example, the Mitigation Directorate estimates that GIS archives may reach petabytes (1,000 terabytes) to support mitigation in the future. While the network will only need to transport a small fraction of the GIS information at any given instant, the bandwidth required may still be extensive. This situation is particularly true if the need is for interactive access to GIS archives and the amount of GIS information to be retrieved in any interactive query is large (e.g., greater than megabytes). Additional bandwidth in the form of two T1s has been proposed and approved between Washington, DC, and Hyattsville, MD (one T1), and between Hyattsville, MD, and Denton, TX (one T1). This is an alternate route in the event of network failure between Washington, DC, and Mount Weather, VA.

3.3.5.4 Modeling and Simulation Support

The U.S. Fire Administration has indicated a desire to evaluate advanced modeling and simulation applications such as 3-D virtual reality. Virtual reality applications will allow realistic simulations of search and rescue (SAR) scenarios or arson scenes so that fire marshals might inspect evidence and safely experience the crime scene for training purposes. This potential requirement implies a need for the target network architecture to be scalable and provide high performance in a number of areas including bandwidth and latency. Local- versus wide-area requirements will also need to be evaluated and refined to ensure the network can provide the required services at an affordable cost. The U.S. Fire Administration's Simulation and Training Network Project (SIMLAB) has made considerable progress during the past two years, since development of the initial *FEMA IT Architecture, Version 1.0*.

3.3.5.5 Exercise Training and Analysis

Another requirement derived from the *FEMA IT Architecture* that the future network will need to support is exercise training and analysis. This requirement includes support for computer-based training, on-line exercises, classroom instruction, and similar multimedia requirements. The Preparedness, Training, and Exercises (PT&E) Directorate is one of the FEMA organizations that needs a properly designed network to support these requirements. Necessary network characteristics include scalable bandwidth and low delays (e.g., latency).

3.4 TARGET NETWORK ARCHITECTURE

3.4.1 Overview

This section identifies and discusses important characteristics and objectives of a candidate target network architecture that satisfies current and future FEMA requirements. Specific technologies and product types to evaluate are suggested and are under active evaluation within FEMA. The

suggestions are based on evaluations of requirements and opportunities, and on the current or near-term availability of mature products and technologies.

3.4.2 Objectives and Criteria

As previously stated, existing FEMA networks work well and satisfy all current mission-critical requirements. Therefore, it is important that any modifications to the current architecture offer significant advantages, cost savings, or new capabilities. The following paragraphs summarize some of the key objectives and criteria that the FEMA ITS Directorate is considering.

3.4.2.1 Cost Effectiveness

The target architecture should provide an early return on investment in terms of lower recurring costs and reduced infrastructure support costs. This potential return can be accomplished, for example, with a reduction in the number of point-to-point T1 circuits required for the backbone voice and data networks. Further infrastructure and support savings could be achieved by integrating voice and data functions in a single platform.

3.4.2.2 Simplicity and Manageability

Complex systems and technologies are difficult to operate and maintain. In contrast, well-designed systems and products are usually easier to integrate and manage. Hands-on product evaluations and working prototypes are some of the best methods of evaluating these criteria.

3.4.2.3 Reliability, Availability, Survivability, and Maintainability

High reliability, availability, survivability, and maintainability are important characteristics of equipment, networks, and supporting systems. Network integration poses additional issues because voice and data networks have traditionally not been held to the same standards. Therefore, it is important to ensure that the target architecture does not degrade the performance of existing networks. FEMA recognizes that it is equally important to engineer affordable systems-level requirements and not arbitrarily impose 99.999 criteria on all aspects of the target architecture.

3.4.2.4 Low Risk, Minimum Downtime

Risk is inherent in any technology upgrade. FEMA engineers are satisfied that the network engineering risk in migrating to a target architecture can be identified and managed. Likewise, equipment and implementation strategies can be designed to minimize downtime during network upgrades and integration.

3.4.2.5 Security

As previously stated, FEMA maintains the security of the voice and data networks by using point-to-point connections, private infrastructure, and firewalls. In addition, the networks are continually monitored and evaluated for security risks.

At the current level of target network architecture development, FEMA has not yet evaluated all the security issues associated with new products and technologies. For example, varieties of security options are possible when using VPNs. Similarly, ATM provides virtual circuit connectivity analogous to physical point-to-point circuits. FEMA will evaluate the architecture and specific security issues well prior to implementation.

The methodology for addressing the security aspects of the target architecture is outlined in Section 2.4 and will be responsive to the requirements of the Critical Infrastructure Protection (CIP) Program.

3.4.2.6 Product Maturity

FEMA recognizes that alternative products should also be evaluated in terms of product maturity. FEMA cannot afford to utilize developmental or beta equipment in the operational networks. Representative indicators of product maturity that will be considered will include *years on the market* and *market share*.

3.4.2.7 Standards, Interoperability, and Legacy Support

Where clear choices are available, FEMA intends to select standards-based products over proprietary products and implementations. The products will be thoroughly tested to ensure interoperability and support of legacy systems. The use of standards will provide more flexibility, increase leverage, and broaden the range of product alternatives.

3.4.2.8 Performance

As a requirement, the target architecture must perform better than or equal to existing capabilities. In addition to standard network performance requirements such as high network availability, new technologies are expected to offer performance-enhancing characteristics as outlined below:

- More efficient bandwidth utilization
- Better dynamic bandwidth allocation
- Bandwidth-on-demand
- Better fault tolerance and recovery
- Graceful degradation.

3.4.2.9 Quality of Service

In the design of the target network architecture, FEMA recognizes that Quality of Service (QoS) is extremely important for the success of integrated networks. QoS must be manageable and measurable. FEMA will address QoS factors at several architecture levels including:

- **Transmission-Level.** Circuits and trunks, bit error, delay, etc.
- **Application-Level.** Voice, data, video, NEMIS, messaging, etc.
- **System-Level.** Manageability, supportability, security, etc.

3.4.3 Evaluation of Alternative Backbone Transport Protocols

FEMA recognizes that several different communications technologies alternatives could be used to integrate the backbones of FEMA voice and data networks (OSI Layer 3 and below). This section outlines some common technologies and alternatives that were considered as candidates for the target network architecture. The last alternative, ATM, is currently being used in the integrated backbone network work in progress.

3.4.3.1 Synchronous Optical Network

Synchronous Optical Network (SONET) is a high speed switching and multiplexing technology. SONET backbones are often used to provide highly reliable transport. SONET offers transmission and self-healing features that are required by telecommunications carriers and large agencies with similar requirements.

A SONET backbone could be used to transport FEMA voice, video, and data traffic. The high-speed, self-healing characteristics of SONET would help increase the robustness of FEMA networks.

Despite the advantages, a SONET backbone is not currently recommended for several reasons. First, FEMA bandwidth requirements are on the low end compared to typical SONET backbone requirements. Second, current switching and routing systems now have characteristics similar to SONET including high availability and the ability to quickly route around failures. Finally, other technologies, like ATM, can perform similar functions with better efficiency due to statistical multiplexing.

3.4.3.2 Frame Relay

Frame Relay is another alternative for data communications. Although Frame Relay is also one of the technologies used to transport voice communications, Frame Relay is not preferred in the FEMA target architecture for two primary reasons. First, scalability is an issue since Frame Relay is typically employed for low-speed links (T1 and below). Secondly, Frame Relay is not the best choice to provide all the required characteristics of an integrating technology in one protocol. For the future, IT architecture applications that have been suggested will require characteristics that include high speed, low latency, low delay variation, efficient statistical multiplexing, and a mature QoS. In order to meet all these requirements, even Frame Relay needs to be transported over ATM, adding additional overhead.

3.4.3.3 Internet Protocol

IP also is not preferred as the common transport protocol for the integrated backbone network. The rationale is similar to Frame Relay in the previous section. IP was not designed to deliver the precise QoS required for integrated backbone transmission of voice and data communications. The Internet Engineering Task Force (IETF) and router vendors are working to improve and standardize QoS over IP. In the future, IP may become a more viable transport protocol for integrated voice, video, and data applications. Note that while IP is not recommended for common

backbone transport, multimedia applications (like voice over IP) will continue to proliferate and increase the need for a high performance backbone with QoS.

3.4.3.4 Asynchronous Transfer Mode

ATM switches are deployed at major FEMA locations across the country. ATM is the only statistical multiplexing protocol specifically designed to integrate the demanding requirements of voice, video, and data traffic streams in a scalable manner (Figure 3-7). ATM addresses several technical issues involved with the integration of multimedia traffic over a common backbone. Most importantly, ATM has mature QoS and traffic management features. Each traffic stream can have a unique set of requirements including bandwidth, delay, jitter, error rate, etc.

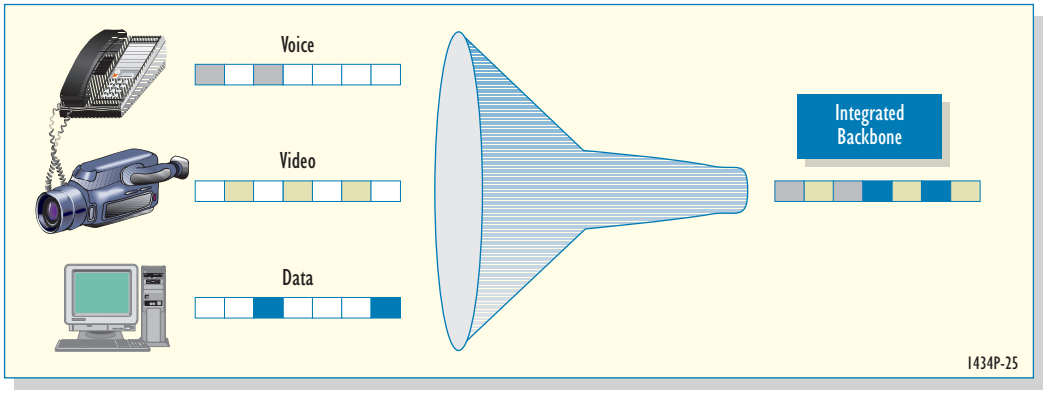


Figure 3-7. Asynchronous Transfer Mode (ATM)

ATM is being used by FEMA because it is easily implemented over dedicated point-to-point links or over more cost-effective leased commercial services. The statistical multiplexing nature of ATM allows multiple types of communications streams to share the same or separate physical connections. Virtual circuits or channels provide pathways for the streams, and advanced QoS mechanisms ensure the streams get the bandwidth and quality required. The potential for ATM also to support virtual circuits and VPNs is of interest to FEMA Regions since it affords future opportunities to establish secure scalable connectivity with States and local governments.

3.4.4 Target Network Architecture Recommendations

The overarching theme of the FEMA target network architecture is *integration*. Corporations, carriers, and government agencies have started integrating their networks at the backbone level and at the services level. FEMA networks can also be integrated; however, integration must be properly designed and accomplished carefully.

The following sections identify new technologies and services that are under active consideration for integration into the FEMA network architecture. Section 3.4.4.3 provides a candidate network transition strategy that is under development at FEMA.

3.4.4.1 Network Architecture

The target network architecture is explained in terms of the two major components: (1) transmission and (2) switching and routing. A few routers have EIGRP running now. The plan is to have all routers running EIGRP by the end of fall 2001.

Transmission

FEMA has a mix of transmission media that include point-to-point, switched services, dial-up, satellite communications (SATCOM), and other wireless media (Figure 3-8).

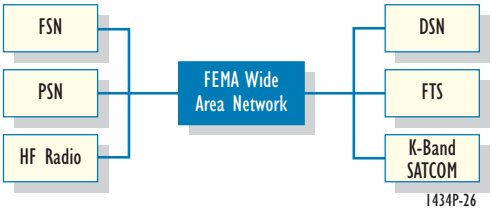


Figure 3-8. FEMA Transmission Media

The primary recommendation for the target architecture is to integrate the separate voice/data transmission circuits. Instead of traditional TDM methods, the preferred transmission protocol is ATM.

With technologies such as ATM, FEMA can significantly reduce the number of transmission links in the backbone and to the field locations, perhaps by a factor of two. The savings in recurring costs can be expected to quickly pay for the initial investment. A detailed network and cost analysis is needed to accurately size the network connections and to determine the new cost structure.

In the target network architecture, FEMA will be able to use QoS features to manage specific connections and types of service. QoS features will be particularly important for voice and other time sensitive traffic. QoS management will be an evaluation criterion in the selection of vendors and products.

In the target network architecture, the protocols and switching equipment must be able to scale to handle all current and projected FEMA requirements. Scalability is important not just for future growth, but also for handling timing-sensitive applications like voice, video, and simulations. As illustrated in Figure 3-9, the target architecture must be able to scale to handle a variety of applications that have been suggested by various FEMA organizations during the development of this initial and updated *FEMA IT Architecture* document. The target architecture must also provide the infrastructure necessary to efficiently support the requirements derived from the *FEMA IT Architecture* discussed in Section 3.3.5, including multicasting and virtual networks.

Switching and Routing

The integration and convergence of voice, video, and data services recommended at the transmission layer are also recommended for inclusion in the target network architecture at the switching and routing layer. Multi-function systems now offer bridging, routing, switching, and multiplexing services in one platform. The potential advantages of single platform systems include the following:

- Reduced equipment counts
- Reduced training time and maintenance costs

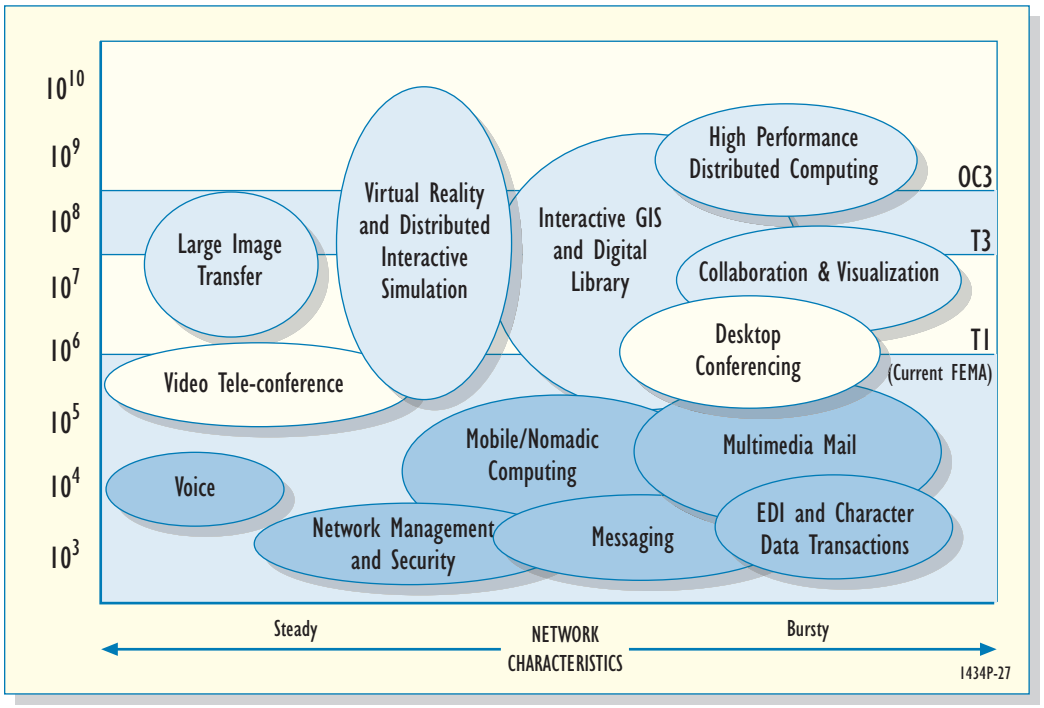


Figure 3-9. Importance of Protocol Scalability

- Faster and easier setup time
- Integrated network management.

Potential disadvantages that will need to be mitigated in the network systems engineering and integration process include:

- Single point of failure
- Less interface options
- Less specialization
- Single vendor.

The single point of failure issue can be mitigated with optional redundant power supplies, hot swappable modules, redundant processor units, etc. Nevertheless, more types of traffic are being concentrated on fewer platforms, which increases the importance of availability specifications. The single vendor issue will be evaluated in the context of performance, cost, service, interoperability, and other factors that influence a decision.

With ATM implementation as the common backbone protocol, other changes in the data routing and switching layers will be evaluated. In particular, there will be an opportunity to maximize switching and minimize routing. Where routing is necessary, one-arm router configurations can be used instead of traditional multi-arm ("milking machine") routers. This configuration will maximize the speed of the network and reduce the number of router hops and the number of

routers necessary in the network. While router performance is always improving, FEMA expects that switches will probably retain cost/performance advantages due to the hardware and software architecture of the devices.

To further enhance the performance of the (data) network, a single Layer 3 protocol and a single routing protocol such as Open Shortest Path First (OSPF) will be considered for incorporation into the network architecture. IP is the *de facto* Internet standard. FEMA anticipates that other protocols, such as IPX, can gradually be phased out in favor of IP. Today, RIP and IGRP are the routing protocols run on all FEMA routers. The transition to a single routing protocol will make routing more efficient and will simplify router maintenance. OSPF is recommended over the existing protocols because it is non-proprietary. OSPF also scales well and is the basis for similar protocols, such as the ATM routing protocol (PNNI).

3.4.4.2 Network Services

In response to the *FEMA IT Architecture* requirements, additional network services are being considered for incorporation in the target network architecture. Note that existing legacy network services are assumed to remain a part of the target architecture:

- **Virtual Private Networks (VPNs).** VPNs offer the potential to increase the reach and flexibility of FEMA networks. Significant cost reductions are also possible. The VPN technology can be IP, Frame Relay, or ATM. An important issue with VPNs is security since VPNs extend private networks over other private and public networks.

  Varieties of VPN security options are possible and are under active consideration. A VPN can be created by tunneling through the public Internet using payload encryption. Alternatively, Internet Service Providers (ISPs) can set up a protected network that does not traverse the public side of routers.

  The VPN options need to be supported by appropriate QoS and Service Level Agreements (SLAs). QoS and SLA provisions need to be independently verified to ensure all service requirements are met. Independent verification is required whether the service technology is ATM, IP, or another technology. In general, the requirements for specifying QoS in FEMA procurements will also need to be developed and understood by FEMA procurement specialists. The Information Resources Board (IRB) and the ITS Directorate appreciate the need to develop and specify new contractual vehicles to acquire a new service.

- **Enhanced Firewalls.** A flexible firewall with high-speed Internet access is recommended for FEMA. Today, FEMA essentially restricts all incoming traffic from the Internet. While this approach is one of the safest firewall alternatives, it may be overly restrictive because the Internet is a cost-effective means of extending the network. The speed of the firewall is also an important consideration as Internet access requirements grow. Security concerns will need to be evaluated to determine the type and configuration of firewalls permitted in the target network architecture.

- **Personal Communications Services (PCS).** Another technology and service that is being investigated and can be integrated with existing FEMA networks is PCS. PCS offers mobile

users the potential of integrating wireless communications, messaging, data, and other useful features. As indicated in *FEMA IT Architecture* interviews with the Regions, PCS technology can be extremely valuable in disaster areas and can also be employed by other mobile users. PCS technology can also be integrated with data services and multimedia services to extend the reach and value of the network (e.g., distance learning).

- **Universal Messaging and Directory Services.** Messaging is a valuable service provided by the voice and data networks. With a universal messaging system, fixed and mobile users can more easily manage their time and resources. Similarly, a universal directory service makes it easier to locate and contact personnel and other resources. FEMA is currently assessing the requirements for messaging and directory services, and the extent to which messaging and directory services can and should be integrated with other services such as paging, PCS, and multimedia services.

- **Support for Thin-Client Networks.** A thin-client approach using technology such as Windows Terminal Server, Oracle Network Computing Architecture, and potentially Java applets presents some interesting opportunities for future systems engineering and integration in a distributed field environment. The fact that FEMA has a number of computers with the Emergency Support Teams and at the DFOs that have to be set up quickly, with short-term users, and managed in difficult environments presents the need for thin-client networks. NEMIS is currently using a Windows Terminal Server.

- **Multimedia Services.** As indicated in *FEMA IT Architecture* discussions across FEMA Directorates, FEMA must plan to support the trend to mixed and multimedia services, networks, and applications. The benefits of enhanced multimedia services include alternate communication channels, visual feedback, distance learning, reduced necessity for on-site travel, etc. As noted previously, FEMA can establish data circuits sooner than voice circuits, thus making multimedia data services a potentially attractive early option for support by the target network architecture.

  Several different capabilities and services fall under the category of multimedia services. A previous section discussed the recommendation for integrated transmission media. This section discusses some of the alternatives under consideration at the application and service layers.

  Computer Telephony Integration (CTI) is one of the fastest growing technology and product areas. With today's technology, it is no longer necessary to always build a local telephone infrastructure and a network infrastructure. Telephones can plug into network outlets or directly into the computer. Alternatively, telephones can be replaced by multimedia-equipped computers. Calls initiated from the data network can be routed over the data network or over the telephone network, depending on the performance, cost, or policies of the agency.

  Video conferencing and desktop collaboration tools and servers need to be provided by the network. While freeware products such as Microsoft NetMeeting work well, the network needs to provide servers and gateways for the best performance. Each capability also needs to be evaluated in terms of network resources required and QoS.

- **Integrated Network and Configuration Management.** As previously described, numerous systems and tools are currently required to manage and monitor FEMA networks. While tools need to be independently evaluated, the target architecture needs to have an integrated network and configuration management capability. Additional network management features that are being considered include:
  — Web-based network management status information
  — Automated IP address management
  — Large screen display facility
  — Automated discovery of network configuration changes
  — Correlation of multiple alarms
  — Automated configuration management.

- **Internet Call Center.** An Internet call center can potentially expand the reach and service of higher-level FEMA functions. Standard services and services tailored to specific scenarios or disasters can be designed. Initially, links can be provided between the current and Internet call centers. Eventually, the call centers should be completely integrated to provide the full range of functions from internal support to disaster services.

- **Alternate Access Methods.** Alternative access technologies such as Frame Relay, ATM, xDSL, and dial-up will continue to be investigated to determine if more cost-effective alternatives could be employed without impact to the mission or flexibility. The standard T1 access strategy works well but may be less cost effective than other alternatives, particularly if the connections need to remain in place for undefined timeframes after the initial installation.

3.4.4.3 Network Updates

FEMA has video conferencing running on the integrated network now. Only one video conference is operational at any specific time due to bandwidth limitations. In the future, FEMA wants the ability to run several video conferences at several locations at once. Several conferences at the same time would bring the network to an intolerable level of service.

Future upgrades include EIGRP on all routers, Variable Length Subnet Masking (VLSM), multicast, and Voice Over IP (VoIP) hopefully by the end of fall 2001.

FEMA has tasked Cisco's ANS division, as part of the Cisco contract, to complete an analysis of FEMA's current wide area network (WAN) with recommendations for the future expansion of all sites outside of the core network to include end nodes and disaster sites.

FEMA has replaced all Cisco 3810s in the core network with Cisco 3640s. This change allowed voice, data, and video over the ATM integrated network. FEMA is planning to roll out new devices to all locations outside of the core network including DFOs after Cisco completes its tasked recommendations.

Denver, CO, was added as a new core integrated network location. FEMA installed a Cisco IGX and 3640 at Denver, CO, in January 2001. The current Cisco IOS that is running on 3640s is IOS 12.1(5) T4. FEMA is currently working on traffic shaping.

3.5 RECOMMENDED IMPLEMENTATION STRATEGY

The FEMA network architecture implementation strategy includes a phased evolutionary approach, prototyping, legacy support, and an event-driven milestone schedule.

3.5.1 Phased Evolutionary Approach

The implementation of the target architecture is being carefully designed to meet FEMA requirements and objectives. A low risk, no downtime approach can be achieved with the use of a limited introduction and overlapping (hybrid) strategy.

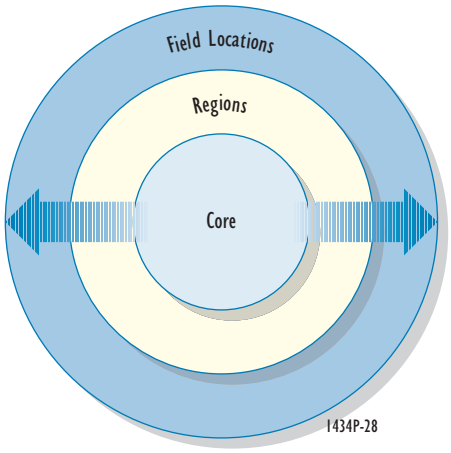


Figure 3-10. Phased Approach Alternative

As shown in Figure 3-10, certain technologies are being considered for introduction in the core, evaluated, and then transitioned to the Regions and field locations. The decision to transition from the core outward will be evaluated on a case-by-case basis. Subject to further engineering analysis, FEMA is planning that the integrated backbone technology be introduced initially in the core of the network. This approach will include selected locations at the top of the network hierarchy including Mt. Weather, Denver, Washington, DC (Headquarters), Hyattsville, Atlanta, Philadelphia, and Denton.

The primary rationale for introducing integrated backbone technology in the core is the potential for higher bandwidth, more aggregated multimedia traffic, and centralized QoS management.

Due to the nature and history of the voice network, careful planning and engineering must be conducted to ensure voice traffic is given appropriate priority and QoS. Similarly, the data bandwidth allocations must be engineered to adequately handle average and peak traffic patterns, as well as mission-critical applications such as NEMIS.

While the integrated backbone technologies are being introduced in the core first, other technologies such as multimedia servers or VPNs will be evaluated. In consultation with the Regions, the ITS Directorate may propose to begin the implementation outside the core due to availability of services, resources, or Regional requirements. The results of Regional and field implementations can then be evaluated for implementation in the core.

In addition to the phased approach, an integrated strategy is also possible for technologies in the backbone and other critical areas. This strategy would allow the technology to be introduced with minimal impact to the existing mission and architecture. This approach would allow operations, management, and support to be thoroughly evaluated prior to full cutover. Cutover to the new technology would then occur after FEMA has accepted the cost/benefit and risk assessment. As an

alternative, this strategy could be maintained indefinitely to provide alternate routing or a cost-effective bandwidth overflow. Figure 3-11 illustrates the current implementation strategy using ATM as the integrated backbone technology.

3.5.2 Prototyping

As an important architectural consideration, FEMA appreciates that vendor specifications and equipment interoperability are difficult to appraise on paper and in limited demonstrations. Consequently, FEMA plans to conduct extended evaluations of new technologies in prototype implementations.

Prototypes will be set up and evaluated in production environments so that cost, performance, and support issues can be realistically evaluated. The prototypes will also be structured to be easily disabled, without impact to the network, during the evaluation period. When the evaluation is complete, the intent is that a prototype can be expanded, removed, left in place, or replaced with upgraded equipment. Figure 3-11 illustrates an integrated implementation concept that can simplify removal or replacement of prototype equipment. For simplicity, only three sites are shown.

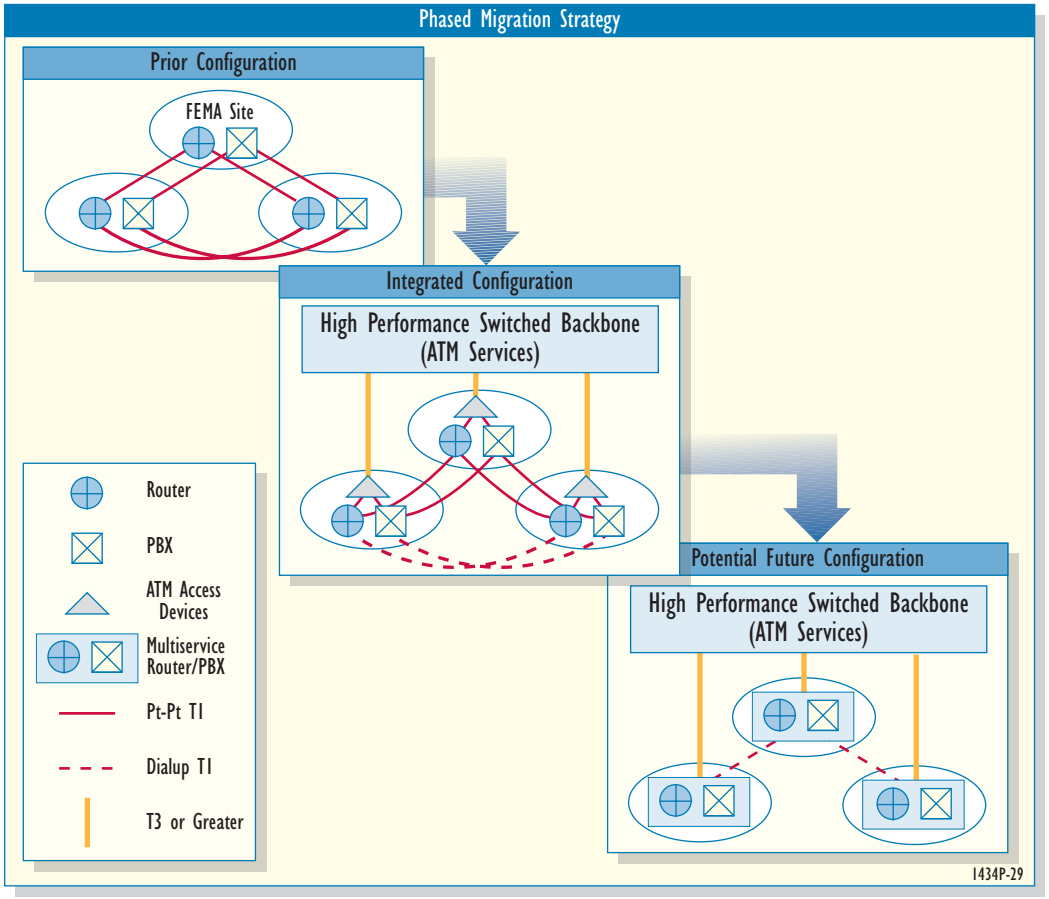


Figure 3-11. Integrated Implementation

In migration to the target network architecture, evaluation plans and procedures will be developed to guide the prototype evaluation process. Features such as Switched Virtual Circuits (SVC), Permanent Virtual Circuits (PVC), and QoS will be analyzed prior to prototyping to determine the preferred implementation and evaluation strategy.

Given the success or failure of the prototype evaluations, FEMA will be able to make informed cost/benefit decisions about full-scale implementations. Evaluation criteria and risk assessments developed in earlier phases will support the selection of technologies and vendors. Network architecture evaluations will help identify the appropriate locations, configuration, detailed systems engineering requirements, and schedule of network modifications.

3.5.3 Legacy Support

At each phase of the network architecture migration, it will be important to maintain legacy systems and networking support. The architecture must support legacy equipment until FEMA consciously and deliberately decides to phase out the legacy systems and equipment.

Prototype evaluations and vendor selection criteria will be developed with legacy support considerations of paramount importance. Because existing PBXs, routers, switches, and associated software cannot be replaced immediately, test plans will be developed to address interoperability issues. Problem detection, troubleshooting, and resolution procedures must be thoroughly tested. Test cases must be developed to stress the network, particularly the interfaces between new technology and legacy equipment.

3.5.4 Event-Driven Milestone Schedule

The FEMA ITS Directorate appreciates that a schedule-driven integration is difficult to achieve with low risk, particularly in an environment with fluctuating budgets. An important architectural consideration is that new technology should be evaluated, prototyped, and phased into the target architecture. As a result, an event-driven implementation strategy is under development and consideration. Section 3.4.2 summarized the most important objectives and criteria. Other significant factors that FEMA is considering in the development of the event-driven milestone schedule are outlined below:

- Independent technology evaluations
- Infrastructure preparations
- Vendor demonstrations
- Initial prototype
- Extended prototype in production environment
- Phased implementation plan (core, Region, field)
- Legacy interoperability testing
- Potential for establishing partnerships with universities and other Federal agencies on the Next Generation Internet (NGI) and Internet2
- Potential for cooperative telecommunications buying services with other Federal agencies.

4. MAINTAINING AND IMPLEMENTING THE *FEMA IT ARCHITECTURE*

4.1 INTRODUCTION

This section provides a discussion of the activities that are required to maintain and implement the *FEMA IT Architecture*. This section also describes the maintenance process in terms of the organizational responsibilities and the change control process. The relationship of legacy systems and new systems to the maintenance and implementation of the *FEMA IT Architecture* is also identified. This section discusses two major requirements. These requirements are:

1. The need to maintain and update the IT and network architecture

2. The need to implement architectural components in new systems, in re-engineered legacy systems, and re-hosted systems.

In maintaining and implementing the *FEMA IT Architecture*, the principles provided in Appendix H shall apply.

4.2 REQUIREMENTS AND PLANS FOR MAINTAINING AND IMPLEMENTING THE *FEMA IT ARCHITECTURE*

The following activities affect the maintenance and implementation of the *FEMA IT Architecture*. These activities are not only applicable to the architecture document itself but also to the associated *FEMA IT Architecture* Data Base. A change in any one of the following activities may necessitate a change to the *FEMA IT Architecture* and the associated Data Base:

- A change in plans such as the *FEMA Strategic Plan*, the *Federal Response Plan*, the *National Mitigation Strategy*, or the *Annual Performance Plan*
- Introduction of new IT or network technology (NT) systems
- Identification of new standards or standard tools
- A change to any FEMA organizational unit mission or business functions
- Identification of new opportunities for systems or applications
- A change in the informational flows of any FEMA organizational unit
- A change in the informational flows and IT infrastructure of a FEMA enterprise business partner to the extent that it has not been standardized and impacts FEMA IT systems
- The addition or deletion of documents or data stores to a FEMA organizational unit
- Changes in plans, policies, and procedures resulting from activities for information assurance as part of Critical Infrastructure Protection (CIP)
- Issuance of new laws, directives, and court proceedings that affect the maintenance and implementation of the enterprise *FEMA IT Architecture*.

4.2.1 *FEMA IT Architecture* Change Management

The *FEMA IT Architecture* is intended to be relatively stable and evolve slowly over time. The architecture is intended to provide a stable and disciplined baseline for the development and implementation of conforming IT systems. Accordingly, major changes to the architecture can expect to be made relatively infrequently.

The Information Technology Services (ITS) Directorate is designated as the primary development and management authority for the *FEMA IT Architecture*. Lead development responsibility is assigned to the ITS Management Division with the close cooperation and assistance of the Program Management Group, the Operations Division, and the Engineering Division. The Configuration Management (CM) Branch within the Management Division is responsible for the *mechanics* of maintaining configuration management controls over the *FEMA IT Architecture*, including document integrity, data base integrity, and digital signature controls. The CM Branch has distributed draft detailed procedures for configuration management to Information Resources Board (IRB) and Information Systems Policy Advisory Group (ISPAG) members, which will also be used for maintenance of the *FEMA IT Architecture* baseline.

4.2.2 Plans for Implementation of the *FEMA IT Architecture*

To implement the target FEMA IT Architecture vision, the Chief Information Officer (CIO) and the ITS Directorate have determined that two ancillary, enterprise-wide guidance documents are necessary. These documents are:

1. ***FEMA Information Resources Management Policy and Procedural Directive (FIRMPD).*** This document already exists but will be rewritten to provide detailed policy and procedural guidance to be compatible with this *FEMA IT Architecture*.

2. ***IT Capital Planning and Investment Guide (CPIG).*** A draft of this document also exists and will be rewritten to conform to the requirements of the *FEMA IT Architecture*. The planning guide is FEMA's internal process and is being developed to be compatible with the Office of Management and Budget (OMB) Capital Planning and Investment Control Process (CPIC).

4.2.3 Legacy Systems Integration

This *FEMA IT Architecture* recognizes that FEMA has a significant investment in legacy systems. It also recognizes that the current IT architecture is substantially meeting current operational requirements. This *FEMA IT Architecture* document sets forth the firm directive that the operation of legacy systems shall not be compromised or jeopardized merely to bring legacy systems into compliance with the architecture. Rather, legacy systems shall be migrated to the target architecture in due consideration of the following major factors:

- What are the necessary resources needed to accomplish the migration, and how do they compare against competing requirements?
- What is the lifetime remaining for the legacy system?

- Are underlying business functions and functional requirements stable?
- What is the operational demand for migration?
- What are the projected cost/benefit savings for migration?
- Is the return on investment for migration justifiable?
- What is the impact on other IT systems?
- What is the projected impact on FEMA networks and communications?
- What is the projected impact on enterprise resources such as personnel, training, hardware, software, data bases, etc.?
- Do FEMA's enterprise partners support the migration?
- Does the proposed migration support evolving mission needs?
- Is the proposed migration in conformance with FEMA IT architectural principles in Appendix H?

4.2.4 CIO and IRB Guidelines for Re-Engineering of Legacy Systems

The CIO and IRB strongly encourage initiatives to re-engineer legacy systems to bring them into compliance with the *FEMA IT Architecture*. An organizational element may propose a re-engineering or re-hosting effort for a legacy system. The proposal should be forwarded to the CIO for consideration through normal business channels. The following guidelines apply:

- The proposal should indicate compliance with the *FEMA IT Architecture* and the architectural principles in Section 1.8. All deviations and exceptions should be noted.

- The proposal should address the questions in Section 4.2.3 to the satisfaction of the CIO and the IRB. The CIO may request that the proponent make a presentation to the IRB describing the initiative and addressing mechanisms for funding it.

- The proposal should indicate compatibility and compliance of the proposed effort with the National Emergency Management Information System (NEMIS) as an architectural component. Any proposed deviations and exceptions from the NEMIS approach shall be justified.

- The proposal should clearly address requirements and plans for cutover and transition to ensure continuity of operations.

4.2.5 NEMIS Infrastructure

FEMA has made a significant investment in the development and implementation of NEMIS. FEMA senior management clearly seeks to leverage this investment across the enterprise. In the development of NEMIS, emphasis has been placed on implementation and integration of advanced IT components. NEMIS has provided a vehicle for FEMA to develop enterprise-wide capabilities with the potential for significant re-use. The successes of NEMIS will directly contribute to the Agency becoming electronic (e-) FEMA.

The NEMIS project is dedicated to evolve as business functions, information flow requirements, enterprise-wide documents/data, and technology evolve. This *FEMA IT Architecture* clearly defines NEMIS as the road leading to e-FEMA. All future IT developments, networking, re-engineering, and re-hosting shall be compatible with the *FEMA IT Architecture*. This means that

consideration must be given to maintaining architectural compatibility with NEMIS or to working closely with the CIO to effect any substantive architectural changes in a mutually agreeable manner. The *FEMA IT Architecture* is open to good ideas and innovation produced by other enterprise systems.

4.2.6 Personnel Requirements for Development, Maintenance, and Implementation of the *FEMA IT Architecture*

Trained and knowledgeable personnel are considered vital for developing, maintaining, and implementing this *FEMA IT Architecture*. Within the ITS Directorate, persons assigned the task of developing, maintaining, and implementing the *FEMA IT Architecture* need the following major skills:

- Understanding of legal requirements contained in public law, directives, and court decisions and their potential impact on IT and NT systems
- Understanding of open systems standards and their implementation
- Clear insight into the FEMA organizational structure and its dynamics
- Established working relationships and partnerships with other Federal agencies, industry, and academia
- In-depth understanding of IT and NT architectural components including business functions, information flows, systems and applications, data and documents, security requirements and services, and advanced technologies
- Understanding of legacy systems at FEMA
- Strong communications skills and ability to bridge FEMA organizational elements in a congenial and cooperative manner to effect beneficial change.

4.2.7 IT Industry Coordination and Liaison

Maintenance and implementation of the *FEMA IT Architecture* demand close IT industry coordination and liaison (1) to identify emerging opportunities, (2) to assess the state-of-the-art, (3) to maintain awareness of industry directions, and (4) to make FEMA's IT requirements clearly known to industry. Consistent with procurement regulations, security, privacy, and confidentiality agreements, this *FEMA IT Architecture* clearly sanctions external industry consultation and outreach activity toward the goals of adopting the best technology for FEMA enterprise-wide architectural components and protecting the critical IT infrastructure.

4.2.8 Partnership with Other Federal Agencies, State and Local Governments, and Voluntary Organizations

FEMA has a large number of partnerships with other Federal agencies, State and local governments, and with voluntary organizations. The *FEMA IT Architecture* supports these partnerships and encourages an expansion of the dialogue. In particular, the *FEMA IT Architecture* encourages additional discussion in the following major areas:

- Potential for increased connectivity via Virtual Private Networks (VPNs) and Extranets
- Agreement on document and data formats (particularly for open systems formats)

- Consensus on standards and standard tools
- Streamlining of information flows to automate wherever possible
- Agreement on electronic information interchange requirements supported by digital certificate services
- Cost-sharing of IT systems, networking, and communications
- Improved methods for maintaining security and document/data integrity
- Improved methods for exploiting the Global and National Information Infrastructure
- Improved approaches and concepts for protecting critical cyber systems and networks
- Increased use of common Commercial Off-The-Shelf (COTS) tools and products
- Shared understanding of the long-term legal and regulatory implications of advanced IT technology
- Sharing of IT lessons learned.

4.2.9 Understanding of Standards

In general, development and maintenance of the FEMA Technical Reference Model and standards profiles require an in-depth and comprehensive understanding of a significant number of information and network standards. It is important to understand the capabilities and limitations of the standards as well as their future direction. An in-depth understanding of the standards is needed to assess COTS implementations as well as to provide a basis for evaluating vendor and contractor proposals. In the system engineering process, an in-depth understanding of standards is also needed to properly specify requirements and not misuse the standard.

This *FEMA IT Architecture* supports collaboration of FEMA's IT professional staff with various standards development committees and authorities to gain increased awareness of standards activities, their direction, and key integration issues. This reflects FEMA's role across the emergency management community as a consumer of standards versus a developer. Participation and collaboration must be approved on a case-by-case basis by the CIO and shall be commensurate with the individual's workload and assigned job responsibilities.

4.2.10 Strategy and Plans for Hiring, Training, and Professional Development

The *FEMA IT Architecture* requires trained and knowledgeable IT professionals capable of working within the lifelines of the enterprise. The high-level strategy and plans for hiring, training, and professional development are briefly summarized as follows:

- To the maximum extent practicable, *FEMA IT Architecture* maintenance and implementation responsibilities will be assigned to current staff members in the ITS Directorate.

- Individuals who are assigned *FEMA IT Architecture* maintenance and implementation responsibilities are encouraged to request additional training as needed.

- All FEMA organizational elements that have significant IT and network development, operations, and/or maintenance responsibilities will ensure that any future hiring or staffing will incorporate personnel requirements and evaluation factors commensurate with this *FEMA IT Architecture*.

4.2.11 Seat Management

One ancillary goal of the *FEMA IT Architecture* is the anticipation that the architecture will establish the primary vehicle for the FEMA ITS Directorate to explore seat management.

Seat management provides a unified service in the way FEMA currently buys desktop computers and support services. Services are paid for on a per seat basis. The seat management concept can allow FEMA to keep pace with technology, eliminate different sources of hardware and software, integration, help desk, and other services; and improve security and reliability. This *FEMA IT Architecture* document supports seat management as an accepted and standardized approach to acquisition of IT resources and architectural components.

4.2.12 Employment of Agency Resources Versus Outsourcing

It is a goal of this *FEMA IT Architecture* that maintenance and implementation activities shall be performed by Agency personnel wherever practicable. Contractor support may be required and will be approved or concurred with on a case-by-case basis by the CIO.

4.2.13 CIO Policies for the *FEMA IT Architecture*

4.2.13.1 CIO Policy on Compliance, Waivers, and Certification

The CIO has determined that compliance with this *FEMA IT Architecture* is mandatory for the development of new IT systems and any proposed re-engineering, re-hosting, or additional development of legacy systems. The CIO has also determined that the architectural principles as stated in Section 1.8 must be followed for FEMA's IT systems. Compliance with the architectural principles shall be verified in all IT systems reviews and audits.

4.2.13.2 CIO Policy on Configuration Management, Configuration Audits, and Configuration Control

The CIO has determined that FEMA shall implement standardized CM services that shall be mandatory for all IT systems to which this architecture applies. The FEMA ITS Directorate has developed a draft set of policies and procedures for configuration management entitled *Draft Technical Review Committee (TRC) and Configuration Control Board (CCB) Guidelines*, dated May 4, 1998. This document is expected to become the basis for disciplined enterprise-wide configuration management. Major CM activities shall include configuration identification, configuration assessment and establishment of baselines, configuration controls, configuration status accounting, and configuration audits. Automated CM tools will be used as appropriate.

As a matter of policy, CM shall be applied in a disciplined and standardized manner across the lifetime of IT systems, networks, data stores, enterprise documents, metadata, business functions, and selected architectural components (such as digital certificates for digital signature).

4.2.13.3 CIO Policy on Allowable Systems Engineering Approaches

As a matter of policy, the CIO has determined that new systems development and any re-engineering or re-hosting shall be performed in accordance with an established and recognized FEMA life-cycle model. All new proposed projects must identify the planned life-cycle model and any planned tailoring. The CIO, in consultation with the IRB, shall verify the assignment of the life-cycle model. On a case-by-case basis, and particularly for mission-critical systems, the CIO may mandate that the proposed project office use formal Software Engineering Institute (SEI) criteria for development.

4.2.13.4 CIO Policy on Information Protection and Security

As a matter of policy, the CIO has determined that information protection and security are vital components of FEMA IT systems or network development, integration, maintenance, and operations. As a matter of high priority, FEMA is currently addressing the requirements for CIP as mandated by Executive Order (EO) 13010 and Presidential Decision Directive 63 (PDD-63). All IT systems and networking development, integration, maintenance, and operations shall be compliant with the approved FEMA Security Architecture that results from that effort.

This page intentionally left blank