FEDERAL EMERGENCY MANAGEMENT AGENCY

# INFORMATION TECHNOLOGY ARCHITECTURE

VERSION 2.0

# THE ROAD TO e-FEMA

EXECUTIVE SUMMARY

MAY 2001

FEDERAL EMERGENCY MANAGEMENT AGENCY

## INFORMATION TECHNOLOGY ARCHITECTURE

## VERSION 2.0

# THE ROAD TO e-FEMA

## EXECUTIVE SUMMARY

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**

3RD ANNUAL
FEMA

# MESSAGE FROM THE DIRECTOR

**THE MISSION** of the Federal Emergency Management Agency (FEMA) could not be more important—reduce loss of life and property from all hazards through a comprehensive emergency management program of risk reduction, preparedness, response, and recovery. To successfully achieve this mission, FEMA depends on vital information services. All of FEMA's central business processes, from disseminating disaster assistance to purchasing office equipment, revolve around information technology systems.

By providing the public, our emergency management partners, and FEMA employees with powerful, efficient electronic (e-) means to interact with us and each other, we will achieve our vision to create an "e-FEMA" that provides better customer service in all areas. Our strategy is to enhance the existing e-FEMA infrastructure, to manage it wisely, and to reuse it whenever possible. Our road map to this goal is this publication, *FEMA Information Technology Architecture, Version 2.0.*

President Bush has said that e-government is a priority for his administration. The President has proposed establishing an e-government fund to support the development of Federal e-government initiatives. All Federal agencies will have to do their part to help achieve these e-government objectives. FEMA intends to take a leadership role and serve as a model agency in fully realizing e-government. The result will be increased citizen access to FEMA and improved delivery of our services to the American public.

This publication affirms FEMA's commitment to e-government and describes what is necessary to achieve the e-FEMA vision. It describes in detail how we are using technology to embrace all aspects of emergency management and organizational performance.

I am pleased to present this document. With the help of all the FEMA family and the necessary resources, we will realize our e-FEMA vision in the next three to five years.

Joe M. Allbaugh
Director

FEMA

# CHIEF INFORMATION OFFICER'S OVERVIEW

**THE FEDERAL EMERGENCY** Management Agency (FEMA) information technology (IT) architecture establishes FEMA's IT as a capital asset to improve the productivity, efficiency, and effectiveness of FEMA's programs. This IT architecture is the foundation of our electronic (e-) government initiatives leading us to e-FEMA.

As FEMA's Chief Information Officer (CIO), I have the responsibility to ensure that the Agency follows all requirements and guidance for the effective management of Federal information resources. With revision of OMB Circular A-130 dated November 28, 2000, sections of the FEMA IT architecture were modified to more closely follow provisions of the *Clinger-Cohen Act* (also known as the "Information Technology Management Reform Act of 1996") and OMB Circular A-11.

FEMA is well-positioned to embark on the road to e-FEMA because of its past and continuing investment in our IT infrastructure and in the National Emergency Management Information System (NEMIS). As the Federal government's Emergency Coordinator, FEMA must be able to set up a fully IT-enabled field office for hundreds of emergency managers, establish high bandwidth connectivity to remote locations and dynamically manage voice, data, and video services for administrative as well as disaster missions. We have the staff and the systems to perform these critical response actions, as well as support the rest of our missions.

NEMIS is FEMA's enterprise application which manages disaster grant funding to individual victims, and State and local governments. This extensive suite of integrated software and hardware has all of the features of e-government and was designed to provide the platform upon which the complete e-FEMA will be built.

As the Director has stated, FEMA's mission is vital to our country. This IT architecture and our continuing progress toward fulfillment of the e-FEMA vision in the next three to five years will greatly improve our ability to serve the country. This publication can be downloaded from the FEMA Web site at http://www.fema.gov, and additional copies may be ordered through the Agency's publication warehouse at 1-800-480-2520.

G. Clay Hollister
Chief Information Officer

# INTRODUCTION

**THE FEDERAL EMERGENCY** Management Agency (FEMA) is the Federal government unit that bears primary responsibility for the nation's emergency management system. When devastation exceeds the capability and resources of local and State governments to respond, States turn to the Federal government for help and assistance. FEMA coordinates Federal disaster relief on behalf of the President, including response and recovery activities of 28 Federal agencies and departments, the American Red Cross, and other volunteer agencies.

FEMA's core business revolves around four major business processes: mitigation, preparedness, response, and recovery.

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 activities require the close collaboration, coordination, and liaison across a broad spectrum of activities at the Federal, State, and local government levels. The vital Grants Management program falls within the scope of the mitigation business function, as well as Geographic Information System products.

Preparedness provides technical assistance, training, readiness, and exercise support. These capabilities help to strengthen community and Tribal readiness through preparedness and strengthen the 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 the disaster, and launch an effective recovery effort.

Response and recovery activities are guided by the *Federal Response Plan*. Response efforts ensure the rapid provision of safe water, food, shelter, and other essentials to disaster victims and assist in the restoration of basic community services from sewage treatment to accessible roads. Recovery efforts aid the long-range restoration of eligible facilities including public roads, bridges, and hospitals. Such efforts support the restoration of economic and community stability.

FEMA manages a Federal program to provide consumer-oriented flood insurance in participating communities. FEMA also provides leadership and support for the nation's fire prevention, control, and emergency medical services activities.

All of FEMA's core business processes require the fastest, most accurate, and most reliable information systems infrastructure available in the civilian sector of the government. FEMA's mission to build, maintain, and operate that infrastructure is materially eased by improved information technology (IT) architecture and design. The target architecture contained in the *FEMA Information Technology Architecture, Version 2.0*, expresses the Agency's commitment to continuously improve the services FEMA provides to the public, FEMA employees, and other Federal, State, and local government agencies. The electronically accessed and delivered services collectively called electronic FEMA or "e-FEMA" are the centerpiece of FEMA's thrust into the early twenty-first century.

FIMA

# e-FEMA VISION

**THIS UPDATED IT** architecture describes FEMA's IT strategy for achieving e-FEMA. It establishes the foundation for FEMA's implementation of e-government. There are numerous incentives for such capabilities, ranging from the Government Paperwork Elimination Act (GPEA) to Presidential Memoranda, General Accounting Office (GAO) reports, industry studies, and customer demands. The e-FEMA vision is best expressed in the following statements:

- IT improves FEMA's capabilities to reduce loss of life and property and to protect our institutions from all hazards
- IT is a strategic resource and force multiplier to improve delivery of FEMA's mission-critical core business products
- IT embraces all aspects of comprehensive emergency management and e-government
- e-FEMA will result in improved services and enhanced solutions for FEMA employees, emergency management partners, and the American public

*FEMA Information Technology Architecture, Version 2.0,* is the road map to e-FEMA. Implementation of *FEMA Information Technology Architecture, Version 2.0*, will place FEMA in the forefront of IT and ensure delivery of the Agency's vital national services. The e-FEMA infrastructure will follow the concept of a seamlessly-integrated IT architecture, implementing the standard of *"Create Once, Manage Effectively, Use Often."*

### e-FEMA Infrastructure

Our infrastructure is technologically current, reliable, and secure. FEMA's IT architecture is based upon the interconnectivity of business processes, information flow and relationships, systems and applications, data descriptions, and technology infrastructure. Emphasis has been placed on providing firewall protection and other security measures to help preserve the integrity of these applications.

The tiers in Figure 1 identify the underlying e-FEMA infrastructure. This is further described in terms of reusable IT architectural components that provide functional capabilities and services that can be integrated into FEMA enterprise-wide and program-centric systems. An architectural component is defined as a high-level building block or piece of a larger system that can be used and reused across multiple systems in a cost effective and standardized manner. Architectural components broadly make up the FEMA IT systems, network, and security infrastructure. Architectural components include IT standards, hardware, networks, software, processes, 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.

The bottom tier establishes sound business processes (including the FEMA Information Resources Management Policy and Procedural Directive [FIRMPD]) and the control capability over all the architectural and system components. This includes operations and maintenance (O&M), effective project management (PM), configuration management (CM), and systems engineering. As technology evolves, and IT and network systems evolve, the need for a disciplined and standardized approach for CM increases. Enterprise-wide CM will allow controlled management of system software, hardware, and related architectural components over time. In order to develop and integrate reliable architectural components for the e-FEMA infrastructure, a set of powerful systems engineering and development tools is required. Computer-aided software engineering tools are intended to be a standardized architectural component.

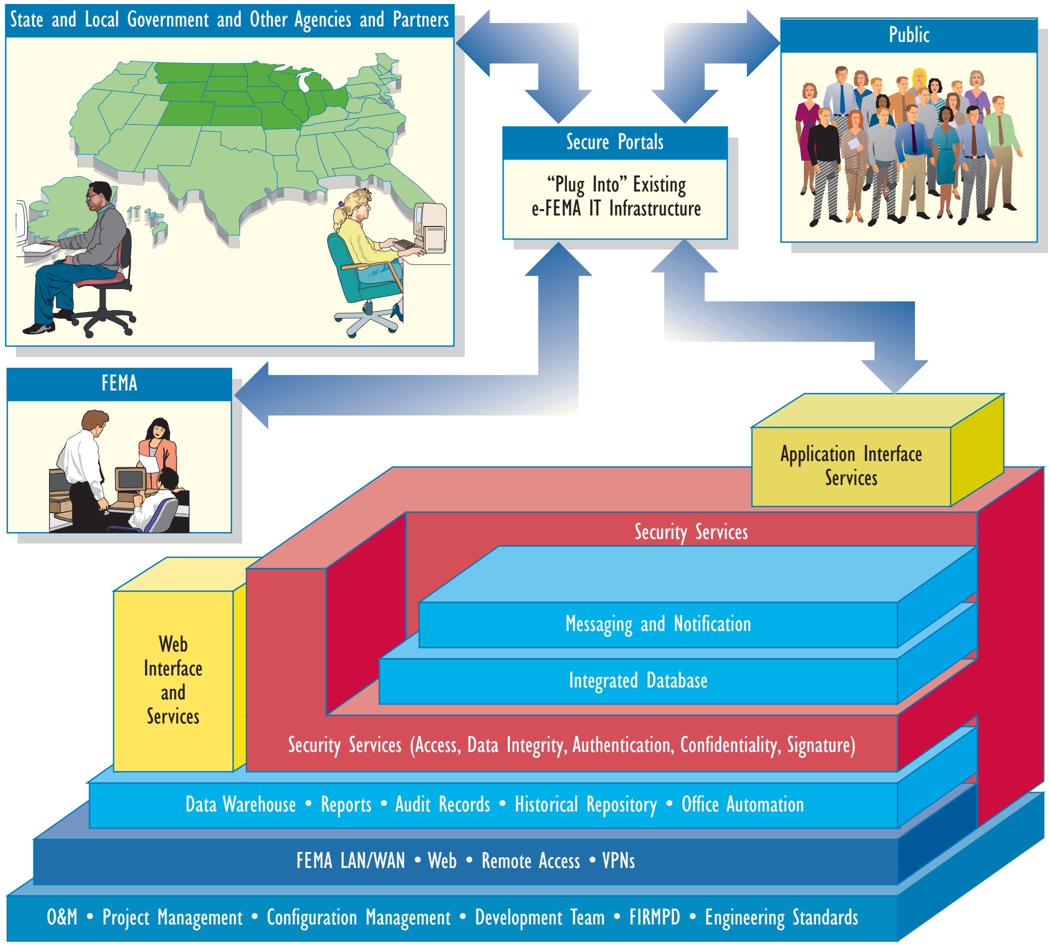

State and Local Government and Other Agencies and Partners
Public
Secure Portals
"Plug Into" Existing e-FEMA IT Infrastructure
FEMA
Application Interface Services
Security Services
Web Interface and Services
Messaging and Notification
Integrated Database
Security Services (Access, Data Integrity, Authentication, Confidentiality, Signature)
Data Warehouse • Reports • Audit Records • Historical Repository • Office Automation
FEMA LAN/WAN • Web • Remote Access • VPNs
O&M • Project Management • Configuration Management • Development Team • FIRMPD • Engineering Standards

Figure 1. e-FEMA Infrastructure

The second tier up represents the communications and network infrastructure. The network consists of several elements: transmission, switching systems, and network equipment. 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. Network services include voice, video, data, and help desk services. Network services will also include virtual private networks (VPNs) and multimedia services.

The third tier shows the high-level approach to data descriptions and document modeling. The tier depicts, from a data and document modeling perspective, how data is maintained (stored/warehoused), accessed, and used. The e-FEMA infrastructure establishes the importance of data and document representation mechanisms for identifying information that can be shared across the enterprise, for minimizing redundancy, and for supporting new systems and applications.

Most of the documents that are in electronic form within FEMA are developed, received, and maintained as office automation files. As the e-FEMA infrastructure continues to evolve, FEMA will gradually move toward an object-relational modeling approach.

The fourth tier shows the network security. FEMA has established a comprehensive information assurance program. 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. Today FEMA restricts all incoming traffic from the Internet and has established a strong perimeter defense. 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.

The fifth tier represents the integration of documents and data. Within the e-FEMA infrastructure, 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 principles of creating documents in their most intelligent form, managing them over their life-cycle, and then gaining maximum downstream reuse, FEMA is carefully moving toward a digital library concept where documents are intelligent, structured, and composed of reusable objects. As this concept is gradually implemented, FEMA will migrate to a formal object-relational modeling approach. This will be consistent with government and industry standards. A key component of the e-FEMA infrastructure is 24-hour per day and 7-day per week (24/7) support for bi-directional electronic messaging and notification services. These services will provide for the receipt, distribution, and dissemination of information including a broad scope of documents and data.

The top tier addresses applications interface services such as FEMA enterprise-wide and program-centric applications (and systems). These are applications that capture, manipulate, and manage the business information to support FEMA's mission operations. This tier also shows the high-level logical dependencies and relationships among FEMA's business activities, which are supported by the applications and systems.

### e-FEMA Application Integration Strategy

Figure 2 shows e-FEMA project application integration within the IT architecture. Currently, there is considerable ongoing effort to develop and integrate a number of distributed enterprise-wide IT applications and systems. The enterprise capability has been established with the National Emergency Management Information System (NEMIS). The e-FEMA foundation has been poured and cured, and we have started other e-government initiatives in many program areas. In the target architecture, e-FEMA projects have secure portals with our partners.

FEMA enterprise-wide systems will be well-integrated and interoperable to the extent identified by the design requirements. All enterprise systems are considered mission-critical and must meet the stated operational factors for the functions that they support. They shall be designed, developed, tested, and integrated in accordance with the IT architecture. They shall also be developed, maintained, and operated to afford critical infrastructure protection and assurance through secure portals as referred to above. In the system development and integration process, FEMA, using its

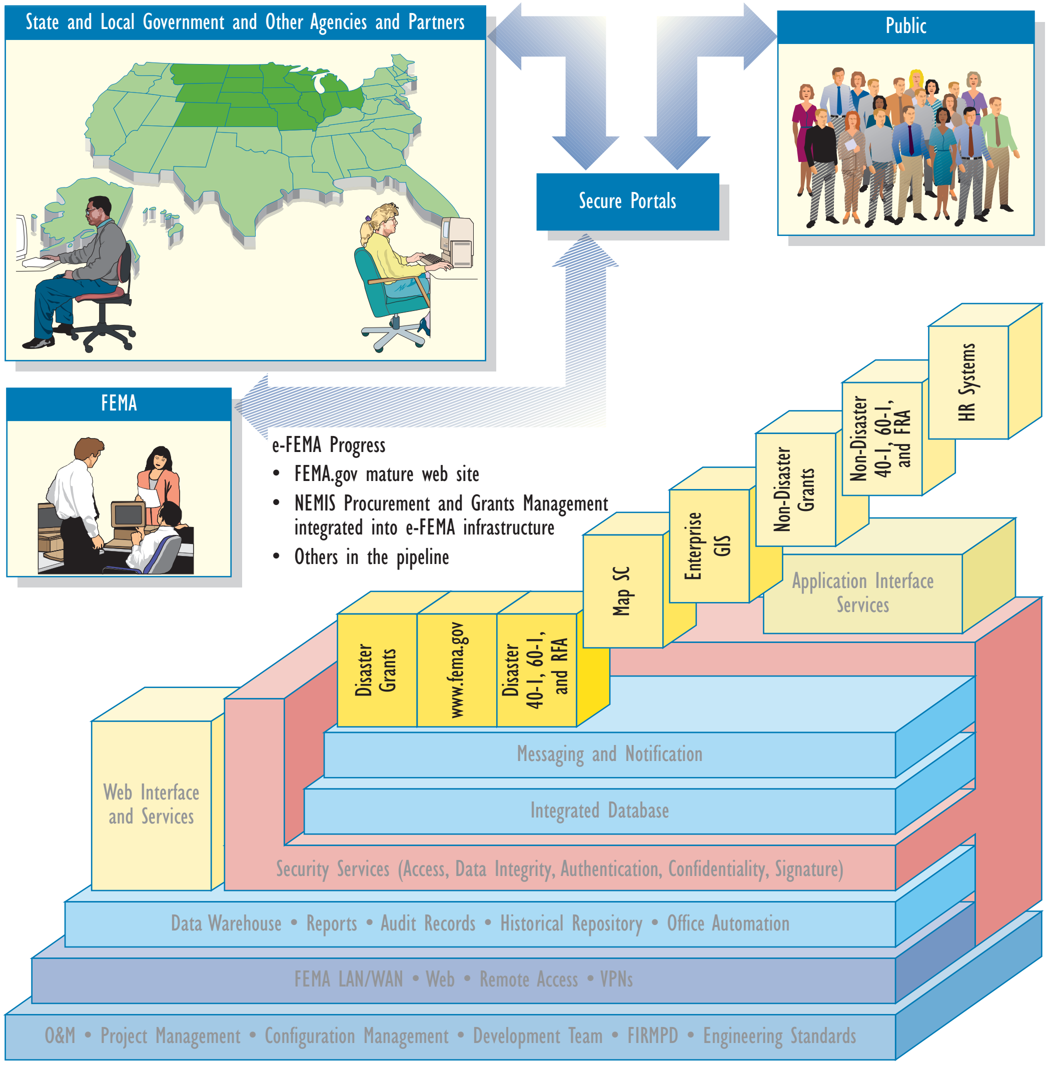

State and Local Government and Other Agencies and Partners
Public
Secure Portals
FEMA
e-FEMA Progress
• FEMA.gov mature web site
• NEMIS Procurement and Grants Management integrated into e-FEMA infrastructure
• Others in the pipeline
HR Systems
Non-Disaster 40-1, 60-1, and FRA
Non-Disaster Grants
Enterprise GIS
Map SC
Application Interface Services
Disaster Grants
www.fema.gov
Disaster 40-1, 60-1, and RFA
Web Interface and Services
Messaging and Notification
Integrated Database
Security Services (Access, Data Integrity, Authentication, Confidentiality, Signature)
Data Warehouse • Reports • Audit Records • Historical Repository • Office Automation
FEMA LAN/WAN • Web • Remote Access • VPNs
O&M • Project Management • Configuration Management • Development Team • FIRMPD • Engineering Standards

Figure 2. e-FEMA Application Integration Strategy

e-FEMA infrastructure, will develop standardized services and capabilities that will be made broadly available to other clients, including users across the enterprise.

As indicated in Figure 2, applications that are completely integrated into the e-FEMA infrastructure are www.fema.gov, disaster grants management, and disaster procurement actions. The Map Service Center achieved its initial component of integration in February 2001. Applications in the pipeline for near term integration include the enterprise-wide GIS system, non-disaster grants management, and the evolving Personnel Resources Information Systems Mart.

## e-Grants

Our platform for implementing disaster e-grants is well established. We already are utilizing NEMIS to automatically process disaster grants. As of January 1, 2001, more than $4 billion in grants have been electronically disbursed using NEMIS. A comprehensive, well-integrated enterprise-wide IT solution for overall FEMA grants management is a top priority for the Agency. This initiative ensures that procedures for grants management, a mission-critical func-

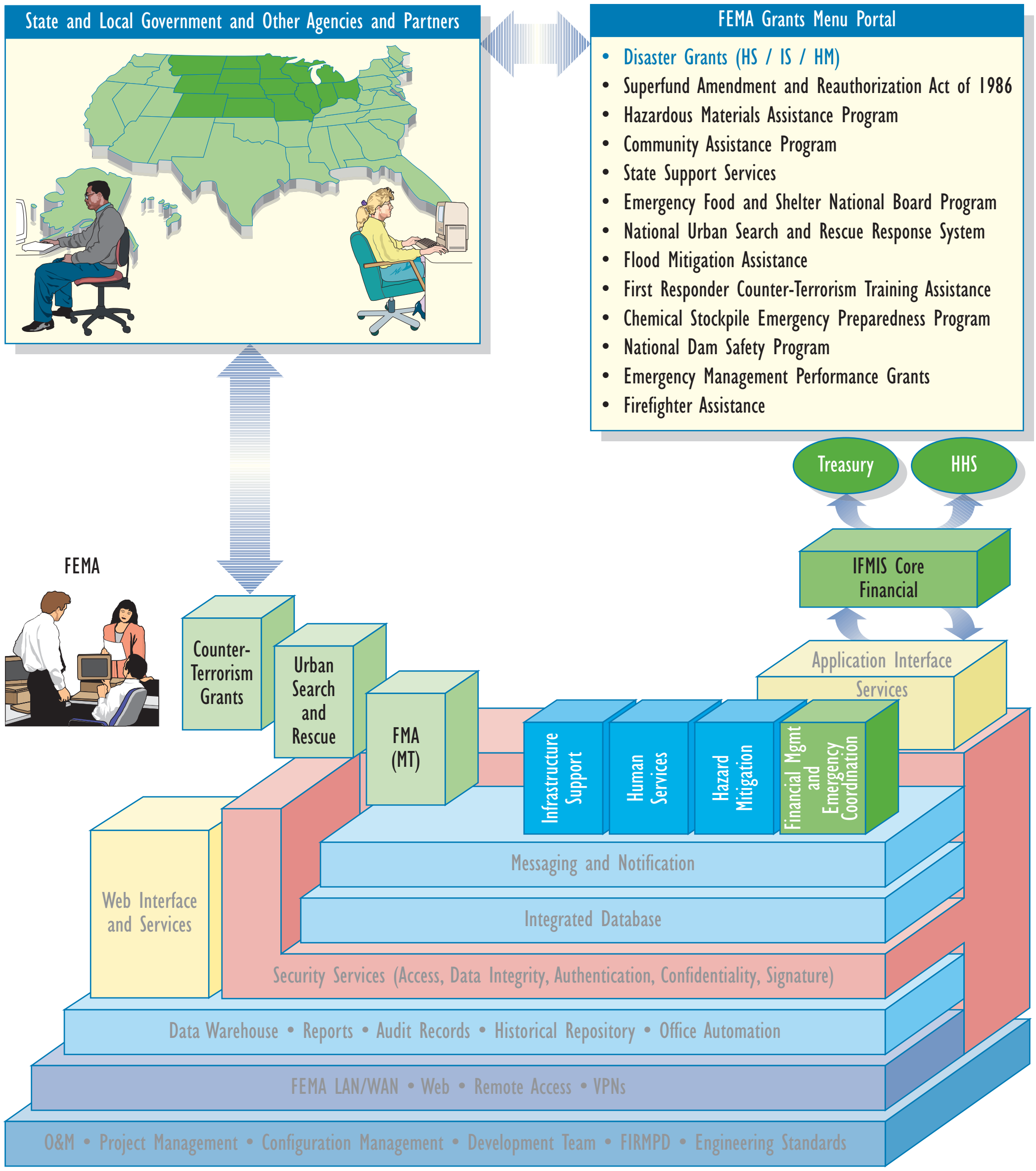

State and Local Government and Other Agencies and Partners
FEMA Grants Menu Portal
• Disaster Grants (HS / IS / HM)
• Superfund Amendment and Reauthorization Act of 1986
• Hazardous Materials Assistance Program
• Community Assistance Program
• State Support Services
• Emergency Food and Shelter National Board Program
• National Urban Search and Rescue Response System
• Flood Mitigation Assistance
• First Responder Counter-Terrorism Training Assistance
• Chemical Stockpile Emergency Preparedness Program
• National Dam Safety Program
• Emergency Management Performance Grants
• Firefighter Assistance
Treasury
HHS
IFMIS Core Financial
FEMA
Counter-Terrorism Grants
Urban Search and Rescue
FMA (MT)
Application Interface Services
Infrastructure Support
Human Services
Hazard Mitigation
Financial Mgmt and Emergency Coordination
Web Interface and Services
Messaging and Notification
Integrated Database
Security Services (Access, Data Integrity, Authentication, Confidentiality, Signature)
Data Warehouse • Reports • Audit Records • Historical Repository • Office Automation
FEMA LAN/WAN • Web • Remote Access • VPNs
O&M • Project Management • Configuration Management • Development Team • FIRMPD • Engineering Standards

Figure 3. e-Grants

tion, enable FEMA and its non-Federal partners to comply with Federal grant management regulations. Efficiency in both disaster and non-disaster grants activities maximizes the benefits of grant funds and supports sound financial management. The ratio of FEMA disaster grant dollars to its overall budget ties this activity closely to agency-wide financial policy and management, making it a sensitive and critical initiative. This existing structure has secure interfaces to FEMA financial systems as well as to financial systems of the Department of the Treasury and other Federal agencies, permitting secure electronic funds transfer. We must now integrate non-disaster grants into this platform.

As indicated in Figure 3, applications currently integrated within e-grants include financial management and emergency coordination, hazard mitigation, human services, and infrastructure support. Flood mitigation assistance integration is near term. Urban search and rescue will be next, followed by counter-terrorism grant assistance.

The following capabilities are being considered for the e-grants systems:

- 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 via electronic means
- Receipting and date-time stamping of the grant application
- Review and collaboration of the grant application
- Tracking, monitoring, and reporting in consonance with the Government Performance Review Act
- Digital library storage and retrieval of documents
- Application of security architecture measures to maintain document and data integrity through secure portals, audit trails, and legal and regulatory records
- Broad information dissemination to get the results out to partners and the State and local levels
- Accelerated financial operations and payments and streamlined assistance for disasters
- Processing enhancements due to Stafford Act changes
- Project closeouts

### e-FEMA Major Successes

**www.fema.gov.** FEMA's primary Internet Web site, www.fema.gov, is the first and most prominent e-FEMA achievement in sharing information on the Internet with the public. As part of established goals to improve customer services, FEMA incorporated the use and capability of the Internet and associated technologies as a viable solution for enhancing delivery of information and implementation of services. FEMA's primary Web site, http://www.fema.gov, contains over 30,000 individual Web pages and provides interactive services through more than twenty different databases. It is the established portal and gateway for Internet users to learn about or access resources pertinent to the Agency's missions. The evolution of FEMA's Web site has been customer driven. Web site design and services are updated to ensure focus remains on expanding capabilities that support goals of the e-FEMA vision and its related e-FEMA infrastructure.

Exponential growth in user acceptance has occurred since the Agency established this public Internet Web site in 1995. During 2000, www.fema.gov received over 150 million hits. The topics of highest interest to visitors continue to be information about disasters and how to take steps to reduce risks associated with disasters.

**NEMIS.** The National Emergency Management Information System is a success story on several different levels. This major FEMA IT application uses the e-FEMA infrastructure. It was developed within 7.5% of its approved budget and has been deployed for just over two years. Its five year development plan was successfully completed in September 2000. NEMIS is a component of this IT architecture and has provided a new technology base to FEMA. As of January 1, 2001, NEMIS has processed over 216 major disasters, emergency declarations, and fire suppression disasters. NEMIS has improved FEMA's disaster operations, reduced operating costs, and reduced by half the time to deliver disaster benefits, such as Individual Assistance (IA). NEMIS has exceeded the goal of 80% auto-determination of IA disaster assistance claims in flooding and hurricane disasters. NEMIS' optical imaging services make documents available to caseworkers within hours of receipt rather than days. NEMIS has brought Federal, State, and local emergency managers closer together in collaborative, real-time decision-making. Following a Presidential Disaster Declaration, NEMIS launches three major disaster assistance grants programs, namely Human Services, Infrastructure Support, and Mitigation. Actions that previously required weeks now take hours.

The effectiveness of e-government depends upon new and improved IT. Our experiences with NEMIS will help FEMA in developing these technologies in the future. Because of the requirements of NEMIS, the e-FEMA infrastructure will be enhanced by providing private and secure communications with States and other Federal partners over the Internet through VPNs.

**Map Service Center.** A measure of notable progress is FEMA's Map Service Center. Over the past twelve months, the Mitigation Directorate's Mapping Modernization effort has been developing an e-government/commerce capability. This new on-line ordering capability, the FEMA Flood Map Store, allows on-line ordering and payment for current flood maps and related products so that businesses can obtain the maps more conveniently. The system went "live" in February 2001. The first stage, which allows FEMA to accept payment for on-line orders, is in operation. The next stage, which will allow FEMA to accept on-line orders from fee-exempt Federal, State, and local government agencies, will be operable in the summer of 2001. This initiative is part of an overall project to build a state-of-the-art Digital Distribution Center at the Map Service Center. During the next year, the Agency hopes to have its maps digitized and available for download from the Internet or via CD-ROM.

The new on-line service makes it easy for customers to identify and immediately place orders for flood map panels. This process used to take days. Business customers will also be able to go on-line to check the status of their flood map orders. The service soon will be available for other groups of flood map users, including individual homeowners. Flood maps are used every time a home is sold to determine whether or not the structure is in an area at high risk of flooding and if flood insurance is going to be required by the mortgage lender. Flood map panels cost a little over a dollar, plus shipping.

The FEMA Flood Map Store has at first simply taken the familiar physical warehouse and created a counterpart in the electronic world. As technology advances, the FEMA Flood Map Store will provide functionality that does not exist in the physical warehouse. More interactive, transaction-based applications will come on-line to create a compelling on-line experience for the user. In addition, the site's security architecture is based upon best practices in the industry and uses the latest available technologies, techniques, and processes.

### Other e-FEMA Successes

The Agency has achieved other successes since publication of the initial IT architecture. These successes include:

- HAZUS' Loss Estimation methodology being applied to all hazards
- The United States Fire Administration's advanced simulation and training for the nation's firefighters
- The Initial Technical Vulnerability Assessments of FEMA's Critical Infrastructure

### e-FEMA Target Architecture Capabilities

Ensuring cost effective integration of FEMA's IT is a continuing task. Improvements in IT have provided the means to reduce costs while providing the services and support required by FEMA employees, emergency management partners, and the American public. As new capabilities are proposed and warranted, they may be approved and added to the Chief Information Officer's (CIO) portfolio. As part of this target architecture, FEMA has identified several e-government capabilities that will contribute to achieving the e-FEMA vision and enhance the e-FEMA infrastructure. Capabilities are listed below and discussed in detail in "FEMA's Target Architecture Capabilities" in Volume 2, Appendix P, of *FEMA Information Technology Architecture, Version 2.0.*

- Enterprise Geographic Information System (GIS) Integration
- Advanced Call Center/Integrated Voice Response
- Next Generation Emergency Operations Center
- Intelligent Collaboration and Visualization Tools
- Wireless Technology
- Virtual Private Networks
- Electronic Publishing
- Distance Learning/Training support systems
- Exercise planning, execution, and evaluation
- Integrated safety management

### Implementation of the Government Paperwork Elimination Act

FEMA submitted its GPEA Plan to the Office of Management and Budget (OMB) in October 2000. GPEA implementation is also an important part of FEMA's emerging strategy in developing e-FEMA.

FEMA's GPEA Plan demonstrates that FEMA is committed to providing improved customer service and efficiency through the use of IT and expanded electronic access to information and transactions. FEMA realizes that providing electronic access options to the public, other government agencies, the private sector, and to internal FEMA staff results in increased customer service and increased awareness of FEMA services. It is anticipated that making FEMA information and services more accessible will result in increased customer access to information and services. In addition, FEMA realizes that as electronic communications technology evolves and becomes more commonplace, and as Internet usage continues to increase, the move to electronic transaction processing and electronic signatures can lead to improved operational efficiencies for the Agency and its partners. In the submission of the GPEA Plan to OMB, FEMA noted that many of the transactions identified are already compliant with GPEA. The GPEA Plan also provides a good project management format that FEMA will use as a checklist to ensure Agency coordination in the continuing move toward e-government, the development of Agency strategic and performance plans, and the integrity of the IT budget process.

# METHODOLOGY AND APPROACH

**AS ILLUSTRATED** in Figure 4, the initial FEMA IT architecture was developed through a series of structured discussions across FEMA Headquarters and Regional staff. The structured discussions mirrored the architectural pyramid discussed by OMB Memorandum M-97-16 and revision to OMB Circular A-130 dated November 28, 2000.

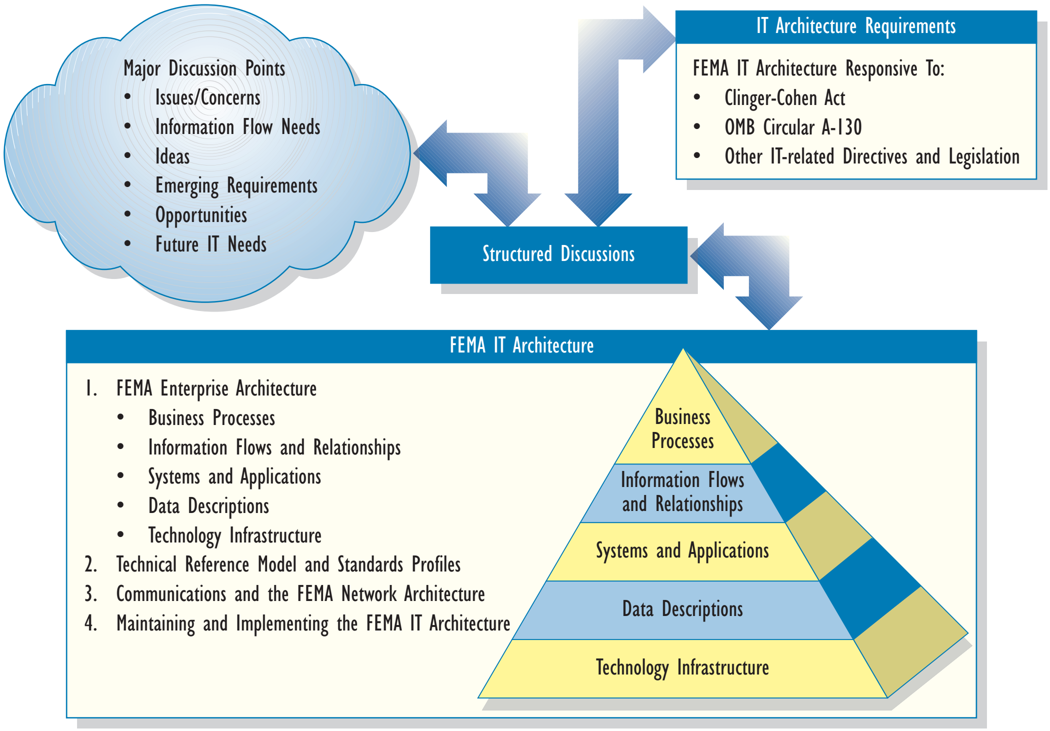

Major Discussion Points
• Issues/Concerns
• Information Flow Needs
• Ideas
• Emerging Requirements
• Opportunities
• Future IT Needs
IT Architecture Requirements
FEMA IT Architecture Responsive To:
• Clinger-Cohen Act
• OMB Circular A-130
• Other IT-related Directives and Legislation
Structured Discussions
FEMA IT Architecture
1. FEMA Enterprise Architecture
• Business Processes
• Information Flows and Relationships
• Systems and Applications
• Data Descriptions
• Technology Infrastructure
2. Technical Reference Model and Standards Profiles
3. Communications and the FEMA Network Architecture
4. Maintaining and Implementing the FEMA IT Architecture
Business Processes
Information Flows and Relationships
Systems and Applications
Data Descriptions
Technology Infrastructure

Figure 4. IT Architecture—Methodology

The e-FEMA infrastructure and application tiers, depicted in Figures 1 and 2, directly correlate to the five layers of the architectural pyramid. The tiers are defined separately but are interrelated and tightly interwoven with the five architectural layers.

Because of FEMA's significant investment in NEMIS, the initial FEMA IT architecture identified NEMIS as an important IT architecture application. NEMIS has been the lead system for providing comprehensive mission support and interoperability. As the catalyst for further implementing advanced IT concepts, NEMIS facilitated development of the e-FEMA infrastructure discussed on the following pages. NEMIS experienced considerable success in the past two years since publication of the initial IT architecture. IT concepts addressed in the current FEMA IT architecture include:

- Developing integrated enterprise-wide systems and services and a common data dictionary
- Developing common and reusable enterprise-wide IT architecture components based on open systems approaches that can be used by both enterprise-wide (total organization) and program-centric (specific program) systems

- Developing, re-engineering, consolidating, and re-hosting selected program-centric systems to be compliant with the architecture and the enterprise-wide data dictionary
- Providing an enterprise approach for systems engineering and configuration management
- Enhancing the FEMA communications backbone to provide improved IT support and improved Quality of Service to the Regions, Disaster Field Offices, and the public
- Exploring the potential for improved connectivity with FEMA's business partners, Regions, States, and local government through establishment of Extranets and VPNs
- Achieving consensus on approaches for creating, managing, using, and interchanging complex documents and data sets in an intelligent manner across the enterprise
- Performing technology insertion in such areas as digital libraries, distributed collaboration tools, distance learning, secure electronic commerce, virtual reality, simulation, and other emerging technologies as added IT support to FEMA business processes
- Developing e-government and e-FEMA

As a matter of high priority and in response to Presidential Decision Directive 63 (PDD-63), the FEMA CIO, in the role of FEMA's Critical Infrastructure Assurance Officer (CIAO), is moving forward on a comprehensive plan for protecting FEMA's critical IT systems and networks. This IT architecture is consistent with that direction and firmly establishes the underlying operational requirements of the Critical Information Protection program. FEMA's security architecture is discussed in a following section of this document.

### Target FEMA IT Architecture

The target FEMA IT architecture is depicted in Figure 5. The architecture seamlessly integrates IT systems, data, and architectural components in a networking and communications environment. The goal of the target architecture is to support the premise of Comprehensive Emergency Management in the areas of mitigation, preparedness, response, and recovery.

The target FEMA IT architecture has the following major characteristics:

- Well-integrated enterprise-wide systems and services
- Improved communications and networking
- Consideration of impact on legacy telecommunications systems as new capability is added
- Adequate bandwidth for advanced IT applications
- Potential for increased connectivity
- Achieving consensus on standards across the enterprise
- Engineering concerns addressed
- Emphasis on open systems standards
- Improved data integrity over the life cycle
- Appropriate security compliance

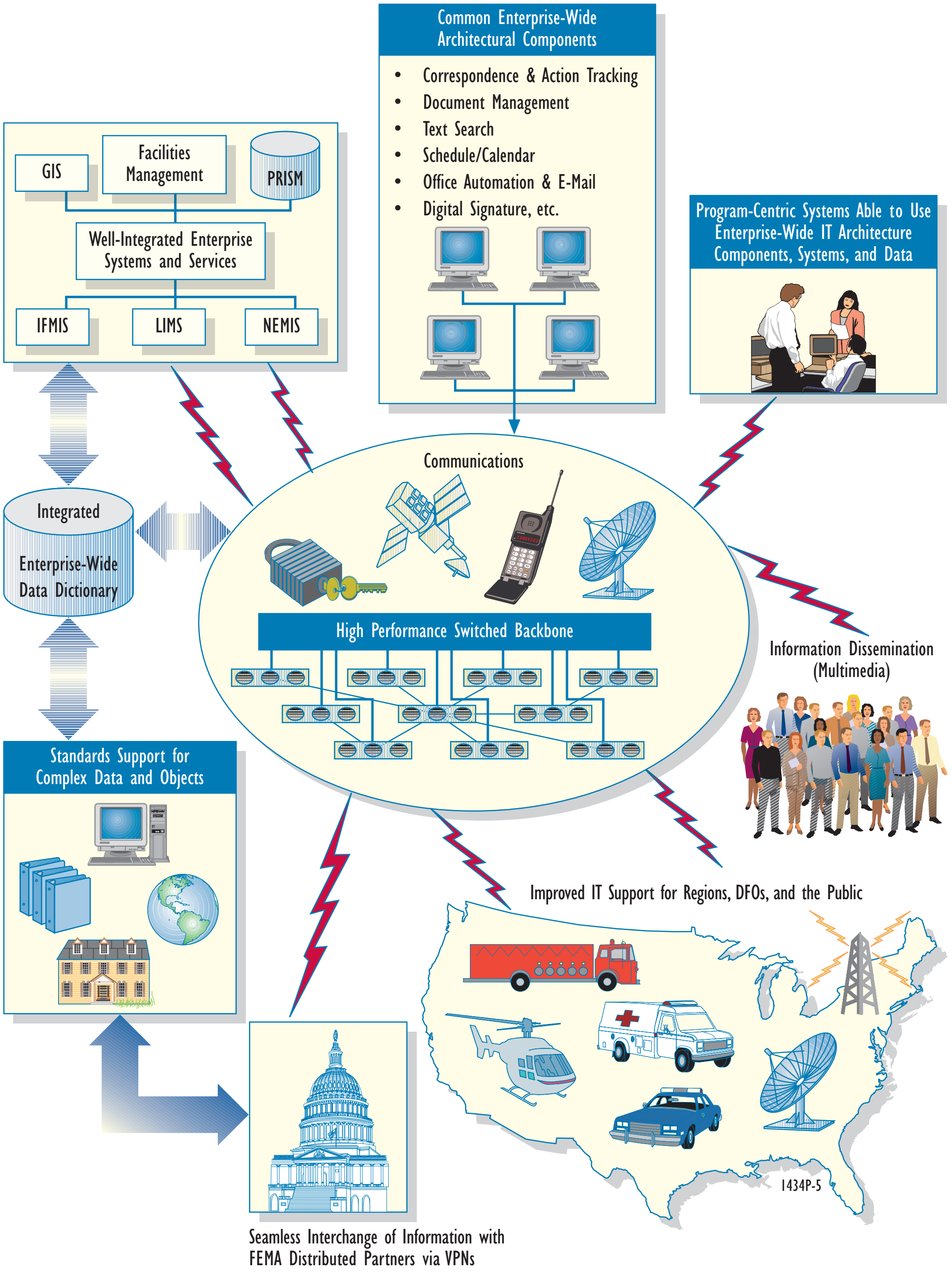

Common Enterprise-Wide Architectural Components
Correspondence & Action Tracking
Document Management
Text Search
Schedule/Calendar
Office Automation & E-Mail
Digital Signature, etc.
GIS
Facilities Management
PRISM
Well-Integrated Enterprise Systems and Services
IFMIS
LIMS
NEMIS
Program-Centric Systems Able to Use Enterprise-Wide IT Architecture Components, Systems, and Data
Integrated Enterprise-Wide Data Dictionary
Communications
High Performance Switched Backbone
Information Dissemination (Multimedia)
Standards Support for Complex Data and Objects
Improved IT Support for Regions, DFOs, and the Public
1434P-5
Seamless Interchange of Information with FEMA Distributed Partners via VPNs

Figure 5. The Target FEMA IT Architecture—Version 2.0

### FEMA Information Assurance and Security Architecture

FEMA clearly recognizes the importance of a comprehensive information assurance program and security architecture, and implementation and development are in progress. In April 2000, the CIAO took the significant steps in protecting FEMA's critical infrastructure, which included the development of vulnerability assessments for FEMA's major IT systems, networks, and physical systems, as well as recommendations for eliminating significant vulnerabilities. This work resulted in the development of System Assessment Reports and System Security Plans, as required by OMB A-130. These documents were completed in November 2000. Additional work will focus on increased monitoring, modem scans, security awareness training, VPN evaluation, and passwords. OMB A-130 also requires that agencies incorporate security into the architecture of their information and systems to ensure that security supports agency business operations and that plans to fund and manage security are built into life-cycle budgets for information systems. FEMA is compliant with OMB Circular A-123, which links agency automated information security programs and agency management control systems. FEMA has also followed the requirements of the *Government Information Security Reform Act*, October 2000.

FEMA's Technical Reference Model, contained in the *FEMA Information Technology Architecture, Volume 1*, provides the high-level guidelines and description of a methodology for the enterprise-wide security architecture. A standardized architectural approach is defined for: (1) identifying required security services for FEMA IT systems and networks, (2) analyzing security implications and requirements for IT systems and networks, and (3) allocating security mechanisms to meet requirements.

The Technical Reference Model also provides high-level security architecture guidelines for FEMA information system developers as they plan for the hardware and software design implementation. The systems developers will 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.

As FEMA continues in its security architecture development, it will follow the proven high-level architectural concepts that have been widely used throughout government and industry. This methodology is responsive to the requirements of PDD-63 to address and analyze security of cyber systems and networks, and the guidelines of the National Institute of Standards and Technology.

### Progress Since Publication of the Initial *FEMA Information Technology Architecture*

In November 1998, FEMA published the *Information Technology Architecture, Version 1.0*, which identified several performance and efficiency enhancements and defined a phased implementation approach. Major near-term recommendations included 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. 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.

Progress was also made in implementing several enterprise-wide systems and programs discussed above. The most significant progress noted is the implementation of www.fema.gov, e-government, and related advances made with NEMIS.

### Performance Measurement for FEMA's IT Systems

What are the key measures that will enable FEMA to run its IT operations most efficiently and effectively? How can such efficiency and effectiveness translate into strategies and tactics that support the real return on the Agency's IT investments that the senior FEMA management, OMB, and the Congress require? IT performance measurement is essential to the CIO in communicating the value of IT and in building the business cases within the Capital Planning and Investment Control Process.

The benefits of IT performance measurements are numerous and include the following:

- Demonstrate immediate improvements in the realization of IT as a value-providing strategic function
- Achieve longer-term value through successful delivery of core business functions
- Build and sustain a business-wise, proactive, and strategic agenda shared by IT and senior FEMA management
- Forge a high degree of participation with top management and the program offices, in their own language—not IT language
- Make IT strategy work and drive the capital planning and resource allocation processes

FEMA is committed to developing specific performance measurements for its IT systems, applications, and services. We have applied IT performance measurements to NEMIS with considerable success. FEMA has developed and is continuing to develop performance measurements for its IT systems, applications, and services in support of the FEMA mission, Strategic Plan goals, and Annual Performance Plan objectives.

### Capital Planning and Investment Control Process

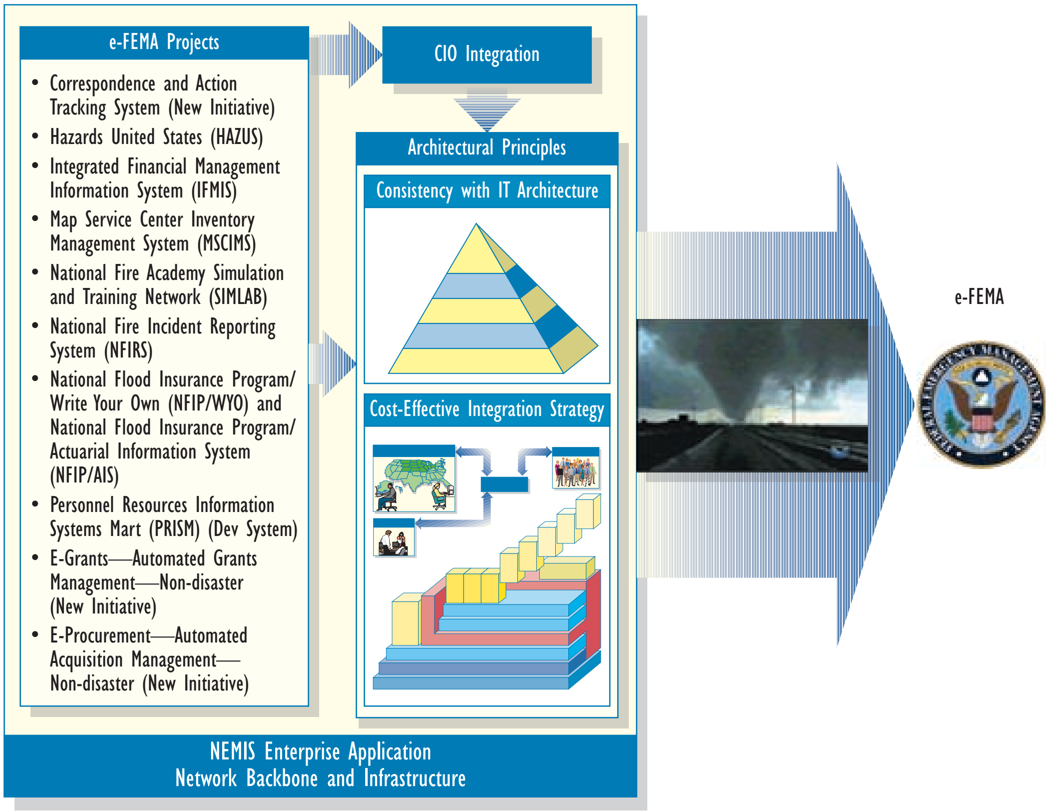
The Capital Planning and Investment Control process was used in developing the current FEMA Target Architecture Capabilities and determining the capabilities that will be part of FEMA's budget submission to OMB. Some of the architectural components and technology require further business case analysis, given the developing state of FEMA networks. For example, advanced groupware technologies such as intelligent collaboration and visualization; integrated voice, video, and data applications; distributed interactive simulation; and distance learning (incorporating virtual reality technology) are widely accepted to be bandwidth intensive in large-scale distributed operations. The current FEMA network is being enhanced but still has limited capability to support some of these advanced technologies. Accordingly, it is important to realize that the FEMA IT architecture provides a framework for discussing how FEMA IT systems might be structured to use common architectural components that are of potential interest across a number of FEMA business units. Business case analyses for some of the more demanding architectural components clearly need to be continued before implementation.

Schnucks
TWA

# CONCLUSION

**FEMA'S MISSION 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 four major business processes: mitigation, preparedness, response, and recovery. These business processes all function through IT.

FEMA has undergone significant IT changes to better meet its mission. FEMA has transformed its corporate culture from "reactive," after-the-fact recovery management to "proactive," responsive management. FEMA's proactive management now actively pursues mitigation measures before disasters occur, monitors threatening events, warns and prepares State and local governments as well as the public, and responds swiftly and compassionately to disaster situations. This transformation will be dependent upon implementation of *FEMA Information Technology Architecture, Version 2.0.* Based upon the implementation of *FEMA Information Technology Architecture, Version 1.0*, FEMA has already transformed its technology base and its disaster operations to be significantly more responsive and effective in mitigation, preparedness, response, and recovery management.


e-FEMA Projects
CIO Integration
Architectural Principles
Consistency with IT Architecture
Cost-Effective Integration Strategy
e-FEMA
NEMIS Enterprise Application
Network Backbone and Infrastructure

- Correspondence and Action Tracking System (New Initiative)
- Hazards United States (HAZUS)
- Integrated Financial Management Information System (IFMIS)
- Map Service Center Inventory Management System (MSCIMS)
- National Fire Academy Simulation and Training Network (SIMLAB)
- National Fire Incident Reporting System (NFIRS)
- National Flood Insurance Program/ Write Your Own (NFIP/WYO) and National Flood Insurance Program/ Actuarial Information System (NFIP/AIS)
- Personnel Resources Information Systems Mart (PRISM) (Dev System)
- E-Grants—Automated Grants Management—Non-disaster (New Initiative)
- E-Procurement—Automated Acquisition Management—Non-disaster (New Initiative)

Figure 6. The Road from www.fema.gov to e-FEMA

### The Road from www.fema.gov to e-FEMA

This IT architecture provides a blueprint and a set of architectural principles for future e-FEMA systems. A number of projects have been identified in the area of e-government. Applications development and integration across the enterprise are the key to success. Cost effective integration strategy is critical. The road to e-FEMA must clearly follow the concept of a seamlessly-integrated IT architecture, implementing the standard of *"Create Once, Manage Effectively, Use Often."* Figure 6 shows the menu of e-FEMA projects along the road to e-FEMA.

FEMA's transformed technology base and responsive disaster operations have positioned FEMA for its next major initiative—creating and institutionalizing e-FEMA. FEMA clearly understands the strategic importance of the Federal e-government and its e-FEMA initiatives. E-government is an increasingly important part of the Agency's strategy to strengthen its emergency management partnerships with other Federal departments and agencies, State and local governments, non-profit and volunteer organizations, businesses, and the public. As FEMA progresses toward achieving e-FEMA, it will be better able to serve FEMA employees, its emergency management partners, and the nation.

This FEMA IT architecture describes FEMA's IT strategy and plans. Fulfilling the Agency's mission demands implementation of e-government by closely linking e-FEMA infrastructure and vision to the public and other government and private agencies. Enhancing the Agency's IT architecture is the prerequisite for its future accomplishments.

COLONY
ESTATES