



# Changing Government Telecom Network Requirements for the 21<sup>st</sup> Century

A FedSources White Paper  
January 9, 2007



## EXECUTIVE SUMMARY

FedSources performed an analysis of the changing needs of federal telecommunications networks and drew conclusions about the kinds of telecom solutions required to meet those needs.

Government needs for telecommunications networks are changing dramatically. The environment in which data must be moved and analyzed is increasingly complex and mission-critical. These needs drive increased service requirements. In turn, these requirements must be met by network equipment and solutions that are “carrier-class.” By carrier-class, we mean characteristics which describe networks operated by telecom service providers such as Verizon, BellSouth and AT&T.

**Hypothesis** – As new challenges emerge in the federal telecom environment, FedSources notes that the telecom network needs of many federal government agencies now resemble the needs of telecom service providers, rather than those of enterprises. Examination of federal telecom network needs in the key performance areas of availability, bandwidth, Quality of Service (QoS), interoperability, and manageability supports this hypothesis.

**Environment** – The current federal government telecom environment has four predominant characteristics: increased network traffic, decreased telecom budgets, increase in network threats, and increase in mission criticality.

**Needs** – The primary needs driven by the current environment include the following:

- **Availability/Reliability:** Agencies such as the Departments of Defense, Homeland Security, Justice, the National Security Agency and Central Intelligence Agency often need 99.999 percent availability. They get it by having diverse or redundant network paths in the backbone and access networks, or by having network equipment with built-in redundancy.
- **Bandwidth:** Agencies need carrier-sized bandwidth, with demand for rates of Optical Carrier-48 or greater, to service metro area networks, military bases, data centers, research/high-performance computing centers, and other sites. Being able to tailor bandwidth rates helps improve cost efficiency and adaptability to the variable demand of planned and future applications.
- **Quality/Prioritization:** It is no longer economically feasible to obtain higher QoS through over-provisioning of bandwidth. Many agencies, like telecom service providers, are converging their multiple networks into integrated Internet Protocol (IP) multiprotocol label switched networks. Federal managers need to customize classes of service for users and applications to give their traffic different precedence on the network. New traffic prioritization capabilities are far more granular than those previously available, providing thousands of separate service queues.
- **Interoperability:** Government agencies operate some of the largest networks in the world, built over time. These heterogeneous networks are difficult to scale and are a barrier to application sharing. Thus, many agencies are migrating to all-IP networks. During this transition (which may take years), the infrastructure must continue to support legacy protocols.
- **Manageability:** Government users, like their large commercial counterparts, want more control over network management, whether it is performed by the service provider or the agency itself. They want greater visibility into network performance and more input into certain tasks like traffic prioritization and administrative changes. Tools need to be usable without excessive requirements for new training.

**Case Studies** – To illustrate the shift toward carrier-class network needs, four case studies of federal telecommunications networks describe the agencies' network needs and the strategy chosen to satisfy the needs. These case studies highlight the following major federal telecommunications networks:

- Department of Justice Unified Telecommunications Network
- Federal Aviation Administration Telecommunications Infrastructure
- Defense Information Systems Network
- Army LandWarNet

## INTRODUCTION

FedSources produced this paper based on a study of the needs of federal telecommunications networks. FedSources' intent is to analyze the government's requirements, describe how they are changing, and to draw conclusions about the kinds of telecom solutions the government requires to meet its network needs.

U.S. federal government telecommunications networks are becoming some of the world's biggest and most complex networks. Such networks have been evolving from multiple, small networks into unified, large, wide area networks (WANs). Some of these agency-wide WANs have thousands of locations nationwide and globally, with certain networks, especially those for national security, involving almost every form of communications technology.

This network convergence drives federal telecommunications managers to adapt to rapidly changing environments. Bandwidth demand is swelling, information technology (IT) budgets are shrinking, physical and cyber threats to networks are increasing, and people are becoming increasingly dependent on their networked applications. To adjust to these new 21<sup>st</sup> century realities, agencies have sought higher performance from their IT solutions – starting with networks. Some of the most important high performance service requirements are shown in Table 1.

Table 1 – Service Requirements Driving the Need for Carrier-Class Telecommunications Networks		
Changing government needs →	Increase service requirements →	For 21 <sup>st</sup> century carrier-class networks
Evolving user needs have increased the demands for the capabilities of government telecom networks	<ul style="list-style-type: none"> <li>• 99.999% network availability/ ultra reliability</li> <li>• Carrier-class bandwidth</li> <li>• Highest quality of service/ traffic prioritization</li> <li>• Interoperability</li> <li>• Manageability</li> </ul>	To build and maintain networks that meet these requirements, government agencies need carrier-class network equipment

Agencies are finding that the performance required from their networks is increasingly similar to characteristics which describe networks operated by telecom service providers such as Verizon, BellSouth and AT&T – known as carrier-class network requirements.

Carrier-class requirements are not easy to fulfill, but are necessary to deliver the network performance needed to support vital federal agency missions in the face of a challenging environment. For many agencies, foregoing these network requirements is not an option. Because of the changing federal IT landscape, more than ever before government telecommunications networks need to be upgraded to carrier-class standards.

FedSources used a wide variety of secondary sources, focusing on materials that demonstrate the evolving needs and requirements of the major telecommunications networks within government. We also conducted primary research, in the form of interviews of current and former government telecommunications program managers and telecommunications industry executives. Quotations that appear in the paper are the result of these interviews.

## FEDERAL TELECOMMUNICATIONS ENVIRONMENT

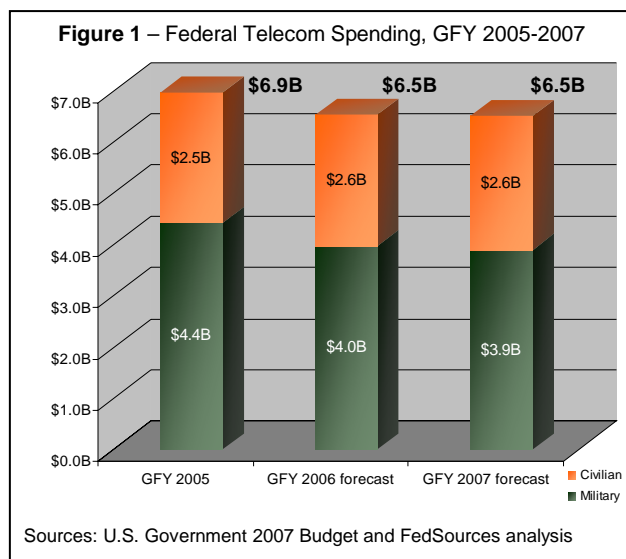
### Increasing Network Traffic

Data bandwidth demand continues to increase and is poised for accelerated growth. Multimedia, high bandwidth services, growing data centers including storage networks, Internet Protocol (IP)-enhanced applications, and Virtual Private Networks (VPNs) are some applications driving bandwidth demand.

Reflecting such demand is the growth in data traffic managed by the General Services Administration's (GSA's) telecommunications contracts, which last year delivered \$1.5 billion in services for the government. Overall business volume (i.e., data and voice traffic) grew 26 percent last government fiscal year (GFY), while voice volume only grew 6 percent. Voice traffic is roughly 30 percent of total traffic compared with 84 percent in 2001<sup>1</sup>. With new bandwidth-hungry applications like on-demand video and imagery, many federal telecommunications decision makers need to re-examine their bandwidth needs to prepare for increases.

### Decreasing Telecom Budgets

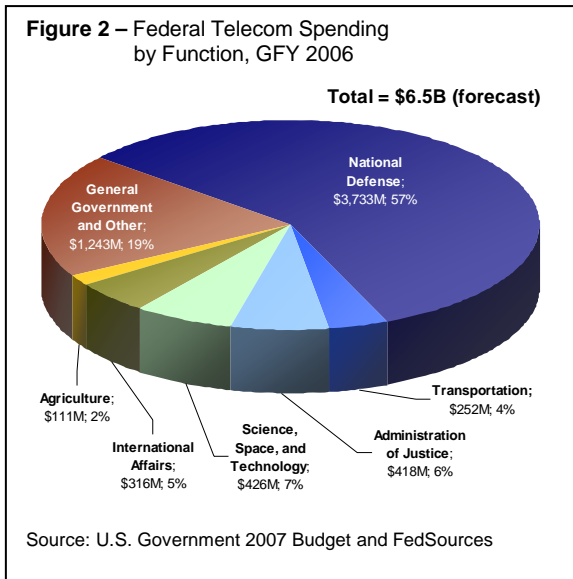
Although data traffic is expected to go up, federal telecom budgets are predicted to go down. FedSources has forecast a federal telecom spending downturn, estimating a decrease from approximately \$6.9 billion in GFY 2005 to \$6.5 billion in GFY 2007 (see Figure 1). The declining cost of telecommunications services is one factor contributing to the decrease in federal telecom budgets, but generally the trend is related to a decline in IT growth rates and an overall slowing of government contract spending. Furthermore, IT budgets are being more carefully scrutinized by agencies' own internal controls (e.g., portfolio management) and external mandates, including the Office of Management and Budget (OMB) Electronic Government (E-Gov) IT Infrastructure Optimization Initiative Line of Business, whose objective is to "further refine the opportunities for IT infrastructure consolidation and optimization, and develop government-wide solutions." Together, these pressures mean that government telecom managers will have to prioritize spending and look for solutions that will help them do more with less.



### Increasing Network Threats

With the ability to cripple the telecommunications service of an entire region, natural disasters, power outages, cable cuts, and software problems have long been the enemies of telecommunications networks. Previously, for the most part, those issues have been manageable risks; however, the Global War on Terror (GWOT), the events of 9/11, Hurricane Katrina, and cyber-crime have heightened federal agencies' concern over network vulnerabilities. During Hurricane Katrina, commercial and public electrical utilities and telecommunications services were overwhelmed, severely degrading agencies' communications, thus impairing their ability to conduct their missions in a time of greatest need. Consequently, now more than ever, federal agencies – particularly civilian – are proactively addressing network shortcomings. As one telecommunication association executive put it, "Civilian agencies are now finding out what the military knew four to five years ago."

<sup>1</sup> Network Set to Boost Federal Network, [Signal Magazine](#), January 2006



### Increasing Application Mission Criticality

Looking more closely at GFY 2007's spending by functional area may give insight into where the federal government's telecom priorities lie. Figure 2 shows spending by government functions. The functional area that accounts for the largest portion of telecommunications products and services is national defense, which includes portions of requirements from all military departments as well as some civilian agencies. National defense, transportation, and administration of justice account for almost 70 percent of all federal telecommunications expenditures. These functional areas are critical to the nation's security and economic interest, and so command greater attention to service performance requirements. Additionally, it is important to highlight that the categories shown in Figure 2 are by function that cut

across agencies. FedSources believes that viewing spending by inter-agency categories is important considering that network and application interoperability among agencies is a strong trend and top priority of many agencies' IT Strategic Plans<sup>2</sup>.

## HYPOTHESIS

As new challenges emerge in the federal telecom environment, FedSources notes that the telecom network needs of many federal government agencies now resemble the needs of telecom service providers, rather than those of enterprises. Examination of federal telecom network needs in the key performance areas of availability, bandwidth, Quality of Service (QoS), interoperability, and manageability supports this hypothesis.

## FEDERAL TELECOM NETWORK NEEDS

### Federal Telecommunications System 2001 & Networx

*"I'd put up the best of our networks against any commercial network."*  
Senior Government Telecommunications Executive

Government telecommunications services generally comprise voice and data network access and transport that are managed by a commercial service provider, with the cost of the underlying network equipment being factored into the price of the services. One current trend is to leave engineering and management to the commercial service providers, enabling the government customer to focus on service definition and strategic planning. Drivers of this trend include government mandates to outsource non-inherently governmental functions (e.g., E-Gov), pressure to reduce operations and maintenance costs, and shortages of qualified technical and managerial personnel.

<sup>2</sup> FedSources analysis of federal agencies' Strategic Plans

Another trend is for the government to acquire its own telecommunications equipment and act as its own systems integrator and/or network manager. This may be necessary when data is mission-critical or there are other pressing reasons why the agency desires more control over the performance of the network. Even when agencies are driving toward service-level agreement (SLA)/performance-based services, they are still concerned and interested in how the infrastructure (i.e., equipment specifications) is put together. With either approach, government agencies gain more control over network performance when carrier-class equipment is deployed.

Federal agencies procure telecommunications services through a number of acquisition vehicles, with the GSA's Federal Telecommunications Systems 2001 (FTS 2001) being the primary contract. Other options include military telecommunications acquisition vehicles and full and open competition in the commercial marketplace.

FTS 2001's replacement contract will be Networkx. Networkx is a 10-year, \$20 billion government wide acquisition contract to be awarded in early 2007 that reflects the new requirements demanded of 21<sup>st</sup> century networks. FTS 2001 offers about 30 core services, while Networkx will expand to 50 services. Networkx will provide all FTS 2001 services in addition to nine IP-based services such as IP VPN and IP telephony, plus optical, professional services, and wireless services.

### **Availability/Reliability**

*"Economy and reliability are equally important – well, in some cases reliability is more important."*  
Senior Government Telecommunications Executive

Network services have become more reliable, faster, and more consistent than what was the standard in 1998 when FTS 2001 began. Thus, agencies are looking for higher service levels, such as 99.999 percent availability which equates to about 5 minutes of downtime per year instead of the 99.8 percent baseline in FTS 2001<sup>3</sup> which is more than 17 hours of downtime per year, about 200 times more.

Table 2 shows the Networkx services that can offer carrier-class availability (i.e., 99.999 percent). Some of the agencies usually associated with needing five nines availability include organizations using classified and emergency networks such as the Department of Defense (DoD), the Department of Homeland Security (DHS), the Department of Justice (DOJ), the National Security Administration (NSA), and the Central Intelligence Agency (CIA).

---

<sup>3</sup> Large Scale Custom Network Solutions Based on FTS 2001: Options and Alternatives, [Telecommunications Review](#), 2006

<b>Table 2 – Network Services With High Performance Metrics for Availability</b> <sup>4</sup>		
<b>Network Service</b> <sup>5</sup>	<b>Functional Description</b>	<b>Availability (“Critical” level of service)</b> <sup>6</sup>
Synchronous Optical Network Services (SONET)	SONET supports digital signals with different capacities, and its inter-working capability enables seamless communications between devices that support dissimilar protocols such as Asynchronous Transfer Mode (ATM), frame relay (FR), and IP. SONET enables agencies to transport voice, data, and video throughout the United States and internationally.	99.999%
Optical Wavelength Services (OWS)	Basic OWS is a point-to-point, bi-directional, single link service delivered over wavelength-division multiplexing (WDM).	99.999%
OWS over the Automatic Switched Transport Network (ASTN)	Basic OWS is a point-to-point, bi-directional service that can be delivered over WDM or ASTN. OWS over ASTN, however, further enables agencies to contract multi-point to multi-point connections in different configurations and classes of service options.	99.999%
Network-Based IP VPN Services (NBIP-VPNS)	NBIP-VPNS provide secure transport of agency applications across the provider’s IP-enabled backbone. Tunnels usually will terminate at the contractor’s edge-router. The three basic NBIP-VPNS solutions are Intranet, extranet, and remote access.	99.999%
Layer 2 Virtual Private Network Services (L2VPNS)	Agencies will be able to acquire point-to-point, point-to-multi-point and multipoint-to-multi-point services. L2VPN services are: Virtual Private LAN Service (VPLS) and Virtual Private Wire Service (VPWS)	99.999%
Storage Services: Network Attached Storage (NAS) & Storage Area Networks (SANs)	Allows data to be accessed through disaster-tolerant systems. High availability Storage Services (SS) include NAS and SANs, which enable an agency to store and access its files from contractors’ data centers.	99.999% (NAS mirrored servers & SAN dual connectivity)

Sources: GSA Network Request for Proposals, 2005-2006 and FedSources analysis

High availability is typically accomplished by having diverse or redundant network paths in the backbone and access networks. For a critical network, an agency may require a dual carrier solution, whereby two vendors deploy duplicate networks. Another strategy is to ensure that network equipment has built-in redundancy in order to meet the most stringent carrier-class reliability requirements.

**Bandwidth**

*“There is never enough pipe!”*

Military Communications Association Executive

Using Network as a proxy for federal telecommunications demand, one can see the government’s broad and demanding bandwidth requirements (see Table 3). Rates range from DS0 (64 kilobits per second (Kbps)) to Optical Carrier (OC)-192 (9.6 gigabits per second (Gbps)). Of the base services examined, all except three services offer bandwidth rates of OC-48 (2.5 Gbps) or greater. From this data one could infer that there is notable demand for carrier-sized bandwidth throughout different parts of the government. Metro area networks, military bases, campuses, data centers, and research and high-performance computing centers are some of the traditional users of large bandwidth. These and other federal users are looking for cost-efficient bandwidth that can easily adjust to and grow with the organization. Being able to tailor bandwidth rates for particular users is as important as bandwidth demand of planned and future applications.

<sup>4</sup> General Services Administration, Network Request for Proposals, August 19, 2005

<sup>5</sup> High levels of availability for other services not listed in Table 2 may be arranged as optional services

<sup>6</sup> Critical service levels are for applications requiring higher levels of availability, performance, or restoral criteria; Routine service levels apply for common government applications

Table 3 – Network Bandwidths for Key Services		
Service	Bandwidth (Access, Port or Transport) <sup>7</sup>	Federal Demand for Service Decreasing ← → Increasing
ATM	T1 – OC-48	←
Private Line	DS0 – OC-192	←
Frame Relay	DS0 – T3	←
Circuit Switched Data Services	DS0 – OC-12	←
IP	T1 – OC-192, 10 Gbps Ethernet	→
SONET	OC-3 – OC-48	↔
Dark Fiber	Less than 12 strands up to and including 192 fiber pairs	→
Optical Wavelength	OC-48 – OC-192	→
Ethernet	10 Gbps	→
Network Based IP VPN	56 Kbps – OC-192, 10 Gbps Ethernet	→
Virtual Private LAN Service	1-1,000 Mbps	→

Sources: GSA Network Request for Proposals, 2005-2006 and FedSources analysis

### Quality of Service & Traffic Prioritization

*“Government takes its responsibility of overseeing the safety and lives of citizens seriously.”*  
Senior Government Telecommunications Executive

To carry out its responsibility for public safety, federal telecom managers need guaranteed levels of service, especially for priority communications and users. Federal telecom services require varying levels of network QoS, as different services tolerate different levels of packet loss, latency/delay and jitter. The strictest QoS guarantees are needed for real-time applications like voice and multimedia; relatively demanding QoS is used by mission critical and transactional applications (e.g., database, enterprise resource planning (ERP), customer relationship management (CRM)); and best-effort QoS suffices for Internet access and e-mail.

Traditionally, services have been provided over separate networks (e.g., IP, Asynchronous Transfer Mode (ATM), frame relay (FR), time-division multiplexing (TDM)), with higher QoS demands often being satisfied through over-provisioning of bandwidth. This is not a cost-effective approach. Today, many agencies, like telecom service providers, are converging their multiple networks into integrated IP multiprotocol label switched (MPLS) networks, which can maintain the QoS levels as expected for traditional services while adding high QoS capability needed by new real-time applications (i.e., Voice over IP (VoIP), video).

As federal telecom services become more numerous, and as the user population grows and diversifies, agencies need more granular traffic prioritization. Federal managers can customize classes of service for users and give their traffic different precedence on the network. Unlike traditional services, new traffic prioritization capabilities are far more granular, providing literally thousands of separate classes of service.

<sup>7</sup> Not all bandwidths are mandatory offerings; Other bandwidths may be available on an individual case basis

**Interoperability**

*“With all the data and application sharing initiatives, agencies not only have to worry about their networks, but they have to think about their partner agencies’ networks too.”*

Former Telecommunications Service Provider Executive

Federal networks are evolving from multiple, small, heterogeneous networks toward singular, large, homogeneous networks. As seen in Table 4, federal networks can be quite large in size. In fact the U.S. Postal Service (USPS) Managed Network Services (MNS) and Federal Aviation Administration (FAA) Telecommunication Infrastructure (FTI) are two of the largest networks in the world. These networks encompass wireline and wireless (e.g., satellite, radio, cellular, microwave) networks.

<b>Table 4 – Select Federal Government Wide Area Networks<sup>8</sup></b>		
<b>Network</b>	<b>Managing Agency</b>	<b>Number of Locations</b>
Non-Secure Internet Protocol Router Network	Defense Information Systems Agency	750-1,000
Justice Unified Telecommunications Network	DOJ	>2,000
Treasury Communications System	Department of Treasury	4,000-5,000
Veterans Integrated Service Network	Veterans Affairs	600-800
FAA Telecommunications Infrastructure	Department of Transportation/FAA	~5,000
Managed Network Services	USPS	~17,000
Bureau of Citizenship and Immigration Services (BCIS) WAN	DHS/BCIS	900-1,100
Homeland Secure Data Network	DHS	500-1,000
Army Reserve Network	Army	>1,000
GuardNet	DoD/National Guard	2,500-3,000
Defense Switched Network	Defense Information Systems Agency	>1,000
Coast Guard Data Network Plus	DHS	~500

Sources: Modeling Internet Protocol Networks, *Sigma*, Winter 2004, U.S. federal agencies, and FedSources analysis

Heterogeneity stems in part from networks being built using the technology available at the time. TDM networks have been the standard for voice services, IP networks for Internet services, ATM and FR for switched data network services, and specialized networks for certain applications like video conferencing.

Two key problems with heterogeneous networks are that they are difficult to scale agency-wide and they present a barrier to application sharing. Expanding or managing separate networks for individual protocols (e.g., IP, ATM, FR, Ethernet) would be prohibitively expensive. Application sharing across different network types is difficult, which is particularly troublesome given federal agencies’ push to share applications and data intra- and inter-agency. To address the scalability and interoperability issues, agencies are migrating to all-IP networks. However, during such a transition, the new infrastructure must support legacy protocols as the migration may take years – since budget cuts, technology developments, interoperating agencies’ and stakeholders’ changing interests, contractor performance, and other factors may affect the network deployment. Certain carrier-class equipment enables legacy protocols and IP/Ethernet to interoperate seamlessly together.

<sup>8</sup> Networks are in various stages of development

## Manageability

*“What keeps me up at night are my worries about single points of failure I don’t know about and not having workarounds established to react if the network fails.”*

Army Telecommunications Manager

Government customers increasingly want visibility into network service levels. Government users, like their large commercial corporate counterparts, want more control over network management, whether it is performed by the service provider or the agency itself. Regardless of who is performing the network management duties, federal customers are requesting greater visibility into network performance and more input into certain tasks like traffic prioritization and administrative changes. When the agency itself is responsible for conducting network management, tools need to be available that existing personnel can use without excessive training – an important consideration given the premium on specialized technical labor.

In light of recent pandemic threats and man-made and natural disasters, there is increased concern about Continuity of Operations (COOP) management. Telecom managers need assurance that network re-routing and restoration occurs transparently after link failure, that backup and disaster recovery between primary and secondary sites happens reliably, and that access for potentially thousands of teleworkers is available on short notice.

As network performance becomes more critical and infrastructure becomes more expansive, there is greater need for network management that provides the federal manager more comprehensive visibility and more simplified management.

## CASE STUDIES

To further illustrate the shift toward carrier-class network needs, four case studies of federal telecommunications networks describe how the current socio-politico-economic environment has affected agencies’ network needs, and strategies used to satisfy those needs. The four case studies are:

- **Department of Justice Unified Telecommunications Network**
- **FAA Telecommunications Infrastructure**
- **Defense Information Systems Network**
- **Army LandWarNet**

---

## Department of Justice Unified Telecommunications Network

### Background

The Department of Justice's mission is to protect America against the threat of terrorism, enforce federal criminal laws, and prevent and reduce crime and violence by assisting state, tribal, local and community-based programs. To better carry out the mission, more information sharing is needed among those program organizations and federal agencies. Greater amounts of information must be quickly and reliably gathered, processed and disseminated in order for law enforcement and litigating parties to better perform their work. Law enforcement is a 24/7 activity, so supporting information should always be available. Personnel are beginning to use real-time information to identify and detain wanted persons, and any delay in data communication increases the potential threat to the safety of the law enforcement official and the public. One of the foundations enabling these critical communications is the DOJ network infrastructure.

In recent years, DOJ networks have been consolidating networks to break down information stove-pipes, reduce operating costs, and improve service levels and security. The major DOJ network consolidation has been the Justice Unified Telecommunications Network (JUTNet), which merges multiple wide area networks. Key DOJ networks include the following:

- Justice Unified Telecommunications Network: Unified DOJ networks
- Justice Consolidated Network (JCON)-S/TS: Secret and top secret networks (e.g., DoD's Secret Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence Communications System (JWICS))
- Criminal Justice Information System (CJIS): Network providing federal, state and local access to major databases such as the National Crime Information Center (NCIC) and the Integrated Automated Fingerprint Identification System (IAFIS)
- Integrated Wireless Network (IWN): Law enforcement voice & data radio system

### Network Requirements and Solutions

JUTNet will service most DOJ components including the Bureau of Alcohol, Tobacco, Firearms and Explosives (BATF), Drug Enforcement Administration (DEA), Executive Office for U.S. Attorneys (EOUSA), Federal Bureau of Investigation (FBI), and the U.S. Marshals Service (USMS). The network will carry classified, sensitive but unclassified (SBU), and unclassified information. JUTNet is expected to transmit information relating to the investigation and prosecution of crimes and terrorist activities; support future voice, video and data services; and increase the agency's existing capability to share information. Because these services are vital to so many DOJ missions, JUTNet's availability, scalability and interoperability are critical.

JUTNet is a managed services contract procured through FTS 2001. Two vendors were selected to build essentially parallel networks to guard against failure in either vendor's network. Vendors will provide redundancy on the backbone network and can also supply dual access to a facility for last-mile diversity. JUTNet will offer this highly available architecture to more than 2,000 locations.

JUTNet will need to supply adequate bandwidth for carrying biometric (i.e., fingerprint) data, wants and warrants, criminal profiles, photos and video. This information will generate significantly more traffic than previous data. Also, the databases for this information are increasingly being accessed by a larger number of federal, state, local and tribal parties – greater dissemination of this information will increase bandwidth demand across JUTNet and related networks. JUTNet will need to provide network access that can appropriately scale to meet users' bandwidth needs.

The previous DOJ circuit-based networks have been a barrier to sharing applications. Deploying new circuits to support an updated configuration of an application and its clients has been slow and costly – point-to-point circuits do not cost-effectively scale with new applications that are required by DOJ components. Replacing legacy circuits with the JUTNet IP network will help solve those application sharing problems.

JUTNet is an IP MPLS network that will replace several DOJ national legacy networks. Those networks have been based primarily on IP over leased lines, ATM and FR circuits. JUTNet's multi-service architecture will support legacy protocols and services until the conversion is complete, without interruption of service.

### **Conclusion**

DOJ's law enforcement mission is especially important in today's GWOT, and the mission has been hampered by stovepiped architectures. As a solution, DOJ has been converging its WANs into a highly available IP MPLS network, with expected benefits of increased application sharing and better scalability and reliability for high bandwidth applications.

## FAA Telecommunications Infrastructure

### Background

A healthy aviation industry is critical to the nation's economic prosperity and national defense. The industry contributes about nine percent to the gross domestic product,<sup>9</sup> and is expected to grow in terms of both passenger and aircraft volume<sup>10</sup>. This year, more than 2 million passengers are expected to fly<sup>11</sup>. The aviation industry supports DoD and National Guard aircraft in their patrolling of the skies and provides airspace monitoring of threats.

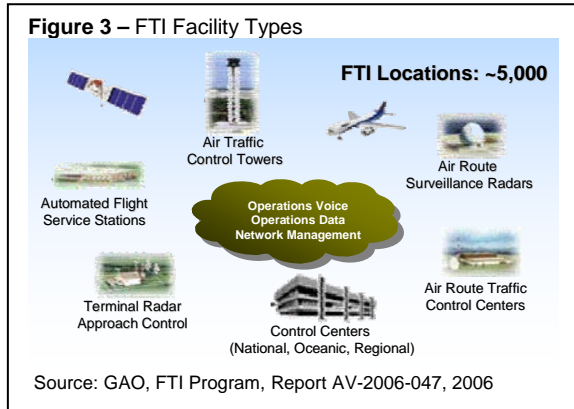
In support of the aviation industry, the Federal Aviation Administration's mission is to provide the safest, most efficient aerospace system in the world<sup>12</sup>. In doing so, FAA must meet the demands of forecasted growth by cost-effectively tripling the capacity of the existing National Airspace System (NAS), which consists of infrastructure (i.e., systems, networks, facilities, aircraft, satellite navigation aids and radars) and human capital. The FAA must also improve its ability to share NAS information among stakeholders, including FAA, DoD, DHS and international organizations, to help ensure a secure and efficient aerospace system. To support these needs, FAA requires 99.999 percent availability for its key communications.

### Network Requirements and Solutions

The NAS' wide area network is the FAA Telecommunication Infrastructure, which is replacing several legacy networks. FTI is considered a mission-critical program because it will carry the National Airspace System's telecommunication services for air traffic control (ATC) operations. A prolonged interruption in FTI could disrupt air traffic or affect related systems and cause significant economic losses or impair national security. Consequently, FTI has some of the most demanding requirements for network scalability, interoperability and availability.

When completed, FTI will consist of about 35,000 circuits for voice, radar and other data links to 5,000 locations (see Figure 3). The FTI lifecycle cost estimate is \$2.4 billion through 2017<sup>13</sup>. FTI's current annual cost is over \$300 million annually<sup>14</sup>.

Legacy networks have had to be replaced because they would not cost-effectively meet the growing operational and mission support requirements. Thus, FTI has been transitioning from traditional dedicated point-to-point circuits to on-demand IP service. FTI is expected to scale better than the legacy networks because of more efficient bandwidth management, simplified provisioning and lower operating and maintenance costs associated with managing one network instead of several. As a GAO analyst said, "The current air traffic control system is based on 1950s-1970s technology – it's not scalable."



<sup>9</sup> General Accountability Office, National Airspace System, October 2005

<sup>10</sup> Federal Aviation Administration, National Airspace System Capital Investment Plan FY 2007-2011

<sup>11</sup> FAA, Aerospace Forecast FY 2006-2017

<sup>12</sup> General Accountability Office, National Airspace System, October 2005

<sup>13</sup> Department of Transportation, Inspector General, FTI Program, Report AV-2006-047, April 2006

<sup>14</sup> House Subcommittee on Aviation Hearing on Air Traffic Control Modernization, June 2006

In the past, NAS communications, mostly radar and voice, have not needed a large amount of bandwidth, although there are facilities that have large bandwidth usage (i.e., en route, large terminal and flight service station). In the future, FAA expects bandwidth requirements to substantially grow. Greater volumes of voice, data and video will go to pilots so they can increase their navigational capability, and to stakeholder sites for processing and sharing. FTI backbone and access providers will need to be able to grow with FAA as NAS implements these new applications.

To smooth the transition to the IP network, FTI will accommodate legacy protocols and various FAA equipment interfaces. FTI will employ multiservice customer premise equipment, so it can manage IP, ATM, Frame Relay and the numerous interfaces FAA has for radar, satellite, radio, modems and other equipment. Ultimately, an all-IP network will help application sharing.

Legacy networks have had little or no integration or interoperability, both barriers to implementing FAA-wide applications. FTI on the other hand is a multi-service IP network that lays the groundwork for new FAA-wide applications. "The Next Generation Air Traffic Control System will give DoD, FAA and DHS a common view of the same information. They currently have their own systems," stated a GAO analyst. An FTI program manager further added, "To share applications, you need IP."

"When it comes to network availability, only DoD can compare to FAA. The way to availability is diversity, and no civilian agency takes diversity as seriously as FAA," noted the FTI program manager. A key pain point regarding diversity, or redundancy, is obtaining last-mile access. Although Synchronous Optical Network (SONET) rings will be at about 350 major sites, getting diversified access for the last mile for many FAA sites is a particular challenge, because of a lack of interest of some smaller local carriers to supply access to what are commonly remote locations, and carrier re-grooming of connections, which often necessitates re-establishing diversified paths. Areas within FAA that need the highest levels of network availability (i.e., five nines) include air-to-ground communications, ground-to-ground voice between facilities, the Wide Area Augmentation System (WAAS), and radar surveillance.

### **Conclusion**

Because the aviation industry is so crucial to the economy and national defense, it is imperative that the foundation telecommunications infrastructure be available, interoperable and scalable enough to meet NAS's current and future needs.

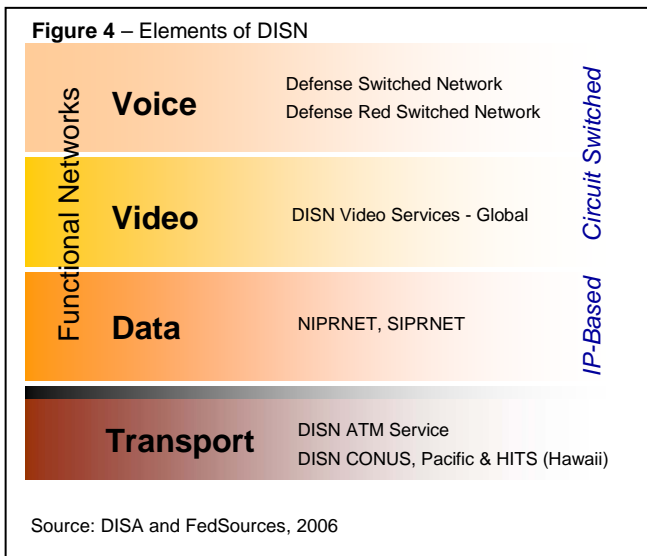
## Defense Information Systems Network

*“When systems fail, people in the theater die.”*

IT Executive and Retired Military and CIA official

### Background

The Defense Information Systems Agency’s (DISA’s) primary mission is to support the war fighter by providing state of the art telecommunications products and services. Central to DISA’s role in providing that support is a program called the Defense Information Systems Network, or DISN. DISN was established in 1991 to consolidate all service and agency IP router networks and is a collection of voice, video and data networks that span the globe. The network encompasses the Defense Red Switch Network, Defense Switched Network, Digital Video Services Global, Secret IP Network and the Unclassified but Sensitive IP Network (see Figure 4).



### Network Requirements and Solutions

The key hardware and software of the DISN are located at more than 400 critical sites across the United States, Europe and Asia. In 2003, DISA released a solicitation for what was then known as the Global Information Grid-Bandwidth Expansion (GIG-BE), now known as DISN CORE. Two of DISN CORE’s main objectives have been to increase the availability of dedicated/owned dark fiber at these locations and to increase bandwidth throughout the network. DISN CORE has achieved both of these objectives first by laying dark fiber to the most critical DISA telecommunications sites and secondly through a migration to optical networking technologies.

The foundation of the DISN CORE’s architecture is an IP optical migration from aging networks. Formerly, the DISN backbone relied heavily on ATM switches and TDM, with inherent bandwidth limitations. DISN CORE’s optical switches use dense-wavelength-division multiplexing (DWDM) to increase the capacity of fiber-optic links and backbone transmission speeds while its high performance routers provide IP routing and MPLS. DISN CORE transport networks include SONET/Enhanced SONET (ESONET) with OC-192 of useable IP dedicated to each site, boosting bandwidth by hundreds of times over former DISN capacity.

### Conclusion

Due to its role as a central piece of telecommunications infrastructure for the war fighter, DISN system and technology requirements are among the highest in government, perhaps in the world. DISN end-users have and will continue to have needs for the highest<sup>15</sup> level of networking services available, especially compared with the system requirements found in enterprise networking at many civilian agencies. Additionally, DISN CORE is vital to war fighters as it is the gateway to the DoD’s global information grid for many other programs and networks such as the Warfighter Information Network-Tactical (WIN-T) and the Joint Tactical Radio System (JTRS), both currently in development.

<sup>15</sup> Highest level of service is measured by Error Free Seconds or Error Seconds, Average Bit Error Rate, Degraded Minutes, Severely Errored Seconds, Residual Bit Error Rate, Availability, Loss of Bit Count Integrity, Delay and Jitter

## Army LandWarNet

### Background

LandWarNet is a term used to describe the Army's concept of enterprise networking and includes all Army networks – from operating and sustaining military bases' IT network infrastructure to communications networks for forward-deployed forces. LandWarNet is the Army's portion of the Global Information Grid (GIG) and is the Army's counterpart to the Air Force ConstellationNet and the enterprise network of the Navy's FORCENet.

While there are many network aspects to LandWarNet, three distinct components or programs have particular relevance as the United States fights its Global War on Terror utilizing the net-centric warfare concept developed by the DoD. These major components include the Warfighter Information Network-Tactical/Joint Network Node (JNN), and the Joint Tactical Radio System.

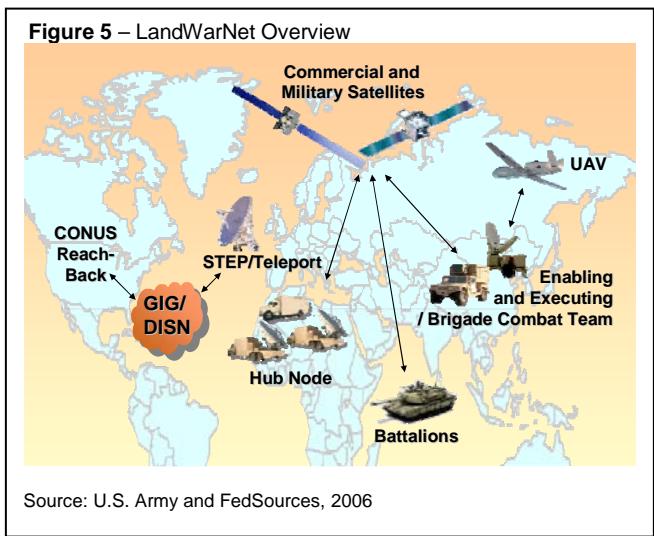
### Network Requirements and Solutions

First, WIN-T and its sister program JNN are mobile, tactical communications systems for brigade through theater level commanders. Like WIN-T and the JNN, JTRS is a fully mobile communications system, but the key difference is that the system is designed for the individual warfighter rather than for a brigade level commander (e.g., walkie-talkie for the soldier).

WIN-T's key enabling technologies will comprise standard elements such as wireless networks supporting VoIP, with support QoS functionality, information assurance and dissemination technologies, and mobile computing. It will integrate JTRS, personal communication devices, and small satellite links.

Capabilities demonstrated through 2006 include on-the-move networking over terrestrial (i.e., line of sight) and satellite (i.e., non-line of sight) links; voice-, video- and data-over-IP; self-healing network properties; satellite tracking and adaptive signal retrieval; network operations with real-time situational awareness; network security; secure cellular communications and collaboration tools reaching from commanders to foot soldiers. A high-level architecture view of the WIN-T and JNN (i.e., LandWarNet) is shown in Figure 5.

In the WIN-T architecture, each network node is considered a point of presence (PoP) complete with a server and router to relay and transmit vital tactical communications. In the WIN-T architecture a network node may be located on a High Mobility Multipurpose Wheeled Vehicle (HMMWV), C-130 aircraft, unmanned aerial vehicle (UAV) as well as the Standardized Tactical Entry Point (STEP) Site. STEP Sites, considered the confluence for reach back communications into the GIG, contain high performance routers and switches. WIN-T communications are transmitted to the STEP Site and in turn transmitted to the continental U.S. (CONUS) via DISN CORE, which is comprised of permanent, high-bandwidth terrestrial pipelines. The key tactical feature of WIN-T is that ability to reach back to CONUS via DISN CORE. This connection using the ultra high speed, high availability DISN CORE will enable the war fighter greater tactical advantage over the enemy.



In a larger sense, WIN-T is one of four enabling technologies in the Pentagon's effort to transform today's military into a smaller, faster, more lethal force. In this vision, WIN-T and JTRS act as mobile battlefield networks and connect to DISN CORE and a space-based network called the Transformational Satellite Communications system, or TSAT.

### **Conclusion**

While availability and reliability tolerances for mobile tactical communications systems are less than that of permanent, terrestrial, high-bandwidth networks such as DISN CORE, WIN-T, JNN, and JTRS must function in a war zone and must survive and thrive in hostile enemy environments. They must endure potential network hacker attacks as well as weather and beyond line of sight issues. This clearly signals a need for high performance equipment, especially at network nodes (e.g., STEP Sites and satellite teleports) that connect the individual network programs to Global Information Grid. It is at these key nodes that require high capacity switching and routing capabilities for multiple protocols and waveforms.

## **SUMMARY**

The sophistication of needs in the areas of availability/reliability, bandwidth, QoS, interoperability, and manageability point to a need for carrier-class solutions. These needs and requirements are illustrated by contract vehicles and programs highlighted in this paper. The new Network program provides for five nines availability and OC-48 or greater bandwidth solutions, reflecting the needs of the government telecom programs. The JUTNet is a convergence of WANs into a highly available IP MPLS network, with the expectation it will increase the ability to share applications, scale properly and provide ultimate reliability for high bandwidth applications. The FAA's Telecommunications Infrastructure exemplifies how a government network that is crucial to the economy and national defense requires substantial availability, interoperability and scalability. The DISN CORE needs the highest level of networking services available, as it is vital to war fighters and is the gateway to the DoD's global information grid for many other programs and networks. Finally, the Army LandWarNet networks must endure network attacks as well as weather and beyond line of sight issues – signaling a need for high performance equipment, especially at network nodes that require high capacity switching and routing capabilities for multiple protocols.

These are just a few examples of the government's increasingly complex telecom network demands. While carrier-class networks may not be needed in every agency, their value is inestimable to the agencies that run applications that are critical to national defense, emergency response, and other areas of national security and economic interest. The breadth and scale of government operations are unmatched by any enterprise. It is clear that many telecom networks built, owned, managed and provisioned by the government have needs that are the most demanding in existence and can not be adequately addressed by enterprise-grade equipment. They are, indeed, carrier-class.