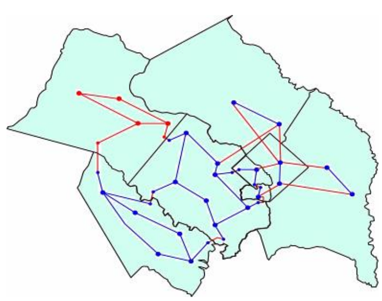
National Capital Region Interoperability Program

The Value and Efficiency of an Inter-Jurisdictional Network: An NCRnet Business Case Analysis

Prepared by NCRIP I-Nets Team
October 2006



ctc technology & energy

engineering & business consulting

Table of Contents

Table of Figures and Tables

1 Executive Summary

This Report presents the results of a business case analysis regarding an inter-jurisdictional fiber-optic and microwave communications network (NCRnet) in the National Capital Region of the United States. This Report was prepared by the I-Nets Team of the National Capital Region Interoperability Program (NCRIP). This Report was prepared in the fall of 2006.

NCRnet is an emerging communications infrastructure designed to support the existing and future public safety and first responder communications requirements between the following entities:

1. Local governments in the NCR, including both counties and municipalities
2. The State of Maryland
3. The Commonwealth of Virginia
4. The District of Columbia
5. Regional first responder groups
6. Regional first responder applications
7. Regional first responder databases
8. Federal first responders, coordinating authorities, and data

The Report addresses the value and efficiency of the emerging NCRnet. Specifically, this Report:

1. Summarizes the existing inter-jurisdictional communications in the NCR and quantifies the potential use of an inter-jurisdictional network—all in terms of the amount of broadband capacity needed to meet requirements (Section 2).
2. Compares and contrasts the lease versus build approaches with respect to:
    - Control
    - Security
    - Reliability
    - Survivability
3. Analyzes the cost of the lease and build approaches.
4. Compares the implementation and operating costs of the build option versus the lease option.

Given the capacity requirements, the build option as envisioned is clearly more cost effective. The build option has an immediate payback[1] when contrasted with the lease option.

- The telecommunications industry is slowly emerging from the voice-only era, and do not have reasonable service rates for high capacity data circuits.
- Leasing circuits leaves the performance and reliability in the hands of a distant provider.

Two cost comparison models are examined in this document, both of which demonstrate that

[1] The annual lease prices, based upon Sprint's GSA rate for dedicated IP service cost, are greater than the implementation costs.

leased services offer less functionality and higher overall costs relative to constructing a private fiber optic network offering far greater functional advantages.

The first model assumes that NCRnet is to meet the full range of application requirements for which it is intended. Under this model, leased services become so expensive that even a year of leased services becomes more expensive than constructing a private network.

The second model assumes a much less ambitious undertaking of supporting only those applications that are already being deployed or currently in used by the jurisdictions. Although this reduces the capacity requirements and associated leased costs to a level that is more palatable, *the cost of a private fiber network would be recouped in just eight years relative to the inferior leased services*. Meanwhile, with the build option, a much higher capacity network is achieved from Year 1, operational costs from Year 8 are more than $300,000 less than the leased solution, and the scalability to support more applications without directly increasing operational costs exists (due to the scalable nature of fiber optics).

This document therefore recommends that the built-fiber option be prioritized where possible over the inferior, more-costly leased circuit option.

2 NCR's Inter-Jurisdictional Capacity Requirements

In the NCR at present, relatively few applications or databases are shared regionally among or across the jurisdictions. Most communications between the jurisdictions occur through meetings, by telephone, via e-mail over the Internet, and by direct access to state and federal databases on dedicated circuits.

This model of regional connectivity cannot effectively scale to support new, emerging uses of technologies in support of life-saving and efficiency-enhancing applications, such as access to multiple streams of interactive video, use of remote data recovery centers, real-time access to graphics-intensive Geographical Information Systems (GIS), and backhaul of wireless communications networks. In addition, the existing model relies heavily on public networks that became saturated during the events of 9/11 and may be impaired or unavailable in a regional emergency.

To address these issues, the communications infrastructure known as the NCRIP "I-Nets" Project, or NCRnet, is designed to provide high standards of performance and reliability over:

1. Dedicated, redundantly routed, fiber-optic and microwave communications
2. High-capacity network electronics
3. 24x7 network monitoring and management

NCRnet will support regional initiatives by providing the communications pathway for enabling access to information and facilitating emergency response procedures that interoperate across jurisdiction lines. NCRnet will support and complement the current regional interoperability programs, including the Regional Wireless Broadband Network (RWBN), the Data Exchange Hub (DEH), and the latest EOC integration applications.

Table 1 and Table 2 illustrate the potential connectivity requirements for each application based on the size and number of jurisdictions.

Table 1: Capacity Requirement Estimates for Each Category

Application	Capacity Requirement (Mbps)				Notes
	Small	Medium	Large	State	
IT Recovery/Backup	194.00	970.00	3891.00	0.00	Assume 1 TB, 5 TB, and 20 TB backups for S, M, L over 12 hour period
Interactive Video	21.50	30.00	37.00	12.00	Tandberg/Web (Fixed 3 Mbps x 4 simultaneous calls per jurisdiction w/ central MCU + 50 to 100 256kbps users; Broadband wireless not included)
One-way Video	150.00	150.00	150.00	150.00	All cameras go to data center (MPEG 2/4)
GIS/CAD/WebEOC	100.00	100.00	100.00	100.00	Data flows from jurisdiction to jurisdiction-- Client-server
Internet	3.00	45.00	90.00	0.00	Redundant T1, fractional DS3, and DS3 Mbps for S, M, L respectively + 50% for encryption
Radio Trunking	1.50	1.50	1.50	1.50	One T1 per jurisdiction
Telephony	1.49	24.83	67.50		Total trunk capacity from each jurisdiction (or assume trunks = 10% users * 90 kbps)
Remote Access/Telecommuting and other additional Internet usage, including Patient Tracking	1.50	22.50	45.00		Additional 50% of Internet bandwidth
Broadband Wireless Backhaul	26.00	65.00	195.00		13 Mbps per base station (S, M, L = 2, 5, and 15 base stations)
Total Capacity Needed per Participant	498.99	1408.83	4577.00	263.50	

Table 2: Total Capacity Requirement Estimates for NCRnet

Application	*Capacity Requirement (Mbps)*				Notes
	Small	Medium	Large	State	
Number of Participant per Category	10	6	3	2	
Total Capacity Needed per Participant	498.99	1408.83	4577.00	263.50	
Total Estimated Capacity Needed per Category	4990	8453	13731	527	
Patient Tracking (non-Internet)	20				20 Mbps In-network/ another 20 Mbps accounted for by Internet traffic
Total Capacity all Jurisdictions (or data centers)	27721 (27 Gbps)				

The following is a brief summary of some of the many functions NCRnet will enable. It is intended to be illustrative only and is not an exhaustive list or discussion.

2.1 Application Usage

NCRnet is designed to support the regional applications requested by NCR information technology and first responder staff during the early phases of the NCRIP project (Table 1). The NCRnet design estimates first-order data capacity needs based on suitable assumptions discussed below. Application priorities differed somewhat from jurisdiction to jurisdiction; however, we find that the usage requirement for a category of applications can be approximated based on the size of the jurisdiction.

For purposes of this analysis, a jurisdiction with 4,000 or more government users is considered "Large," and includes the District of Columbia, Fairfax County, and Montgomery County. Between 1,500 and 4,000 is "Medium," and includes Frederick County, Loudoun County, Prince George's County, Prince William County, Arlington County, and Alexandria. Fewer than 1,500 is "Small," and includes Bowie, College Park, the City of Fairfax, Falls Church, Gaithersburg, Greenbelt, Manassas, Manassas Park, Rockville, and Takoma Park.

2.2 Video Communications

The jurisdictions almost uniformly believe that a variety of video applications are among their most pressing communications needs and believe that NCRnet could enable and support those needs.

2.2.1 Interactive Video

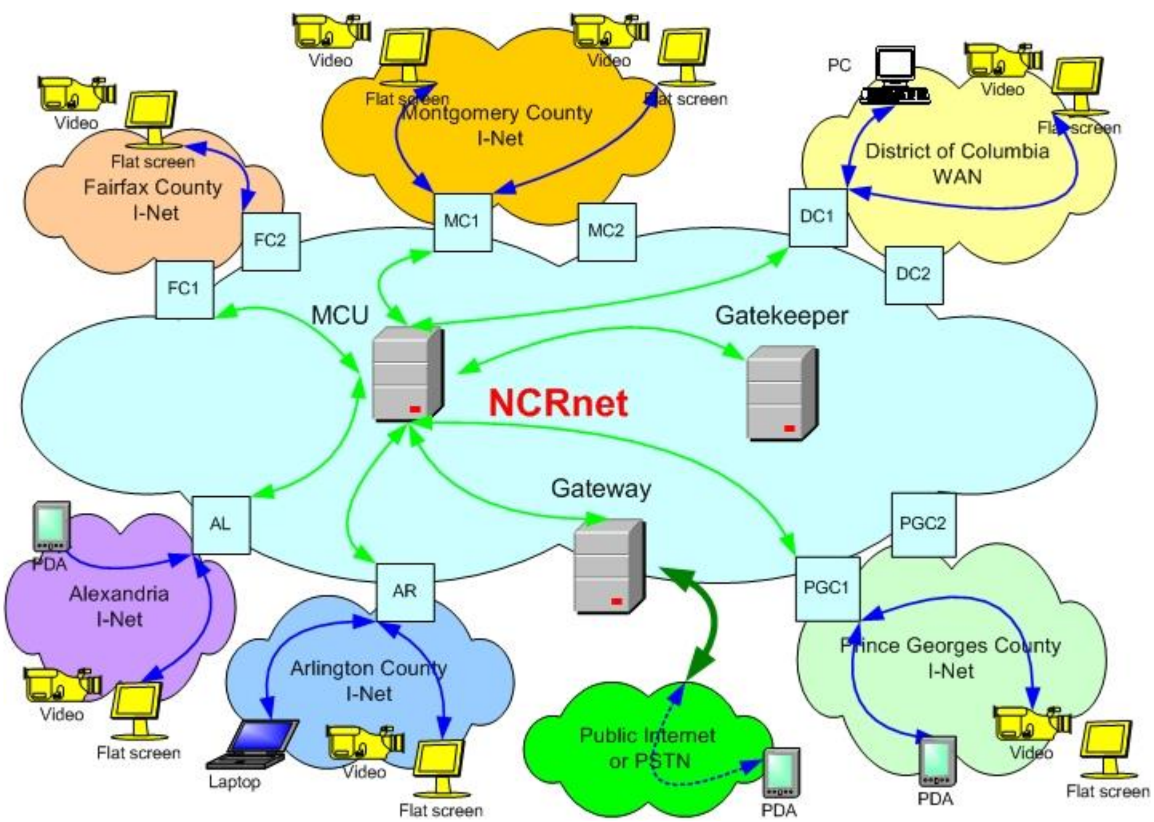
In particular, the jurisdictions express a need for two-way interactive video conferencing among and between jurisdictions. Video conferencing is needed between emergency operation centers, emergency communications centers, and between mayors or county executives/managers. It is also needed in conference rooms for routine inter-jurisdictional meetings, in traffic management centers, and in the field with first responders.

In conference rooms and operation centers, the standard is typically H.323, requiring up to 3 Mbps per session for high-quality video. Some of the video can be Web-rate video, especially in the field or to desktops. Acceptable quality may be achieved using H.323 at as little as 256 kbps, although a much lower spatial resolution and frame rates relative to higher bandwidth sessions.

A large jurisdiction may have one or two inter-jurisdictional meetings during the busy part of a routine day, or quite likely three or four during an emergency situation corresponding to logical groupings of Emergency Support Functions (ESFs) (such as public safety, infrastructure support, public information, and emergency management). Assuming a videoconferencing system architecture that leverages central control resources for multi-seat calls, this could equate to approximately 9 to 12 Mbps bi-directionally per jurisdiction for large collaboration sessions in which all counterpart ESFs in all NCR jurisdictions are involved. Particularly in an emergency situation, another 50 to 100 staff on average, such as first responders or people working on joint projects, may be using lower-quality video accounting for an additional 12.5 to 25 Mbps of video traffic. This does not include mobile videoconferencing participants accessing NCRnet wirelessly, which will be included in the aggregate estimated bandwidth to be provided by this wireless infrastructure.

Figure 1 depicts an example multimedia (including voice and video) conferencing architecture based on H.323. Various different end devices such as PCs, video conferencing equipment, cell phones, and PDAs are depicted. Conferencing is possible between locations within the communities, between communities, and with personnel outside the immediate NCR through the public Internet or the PSTN. The Multipoint Control Unit (MCU) controls the multimedia data flow between the various conference participants while the Gatekeeper provides admission control. The gateway interfaces with external networks and provides the necessary transcoding and interface functions.

Figure 1: Example Video H.323 Conferencing Connectivity



2.2.2 One-Way Video

Viewing of one-way video is another frequently-mentioned requirement. One-way video feeds include traffic cameras, security surveillance, emergency announcements, press conferences, television news, and training video. It may also include backhaul of regional emergency programming to preempt programming on local government access channels. For live video, we assume the use of IP-multicasting, minimizing the bandwidth requirement by ensuring only one “copy” of any available video stream is provided to a given jurisdiction regardless of the number of users accessing the stream within the jurisdiction. For stored, “on-demand” video, we assume of media servers at data centers from which each client accesses video files, though these servers could potentially be distributed to individual jurisdictions to minimize the traffic across NCRnet.

The largest routine one-way video need is for traffic cameras. Montgomery County, the State of Maryland, and the State of Virginia all have more than 100 traffic cameras. Within NCRnet, full-motion video could be transported in MPEG-2 format typically at approximately 5 Mbps. In an emergency, many operations centers will need to view out-of-jurisdiction traffic video, as well as informational video sessions. Assuming twenty out-of-jurisdiction camera feeds for each jurisdiction on average, an additional 100 Mbps will need to flow inbound to jurisdictions.

Regular training and viewing of informational programming may require another ten separate sessions entering a large jurisdiction at a time; therefore 50 Mbps inbound, assuming use of multicast routing or unicast on-demand sessions.

2.3 Voice Communications

2.3.1 Radio Trunking

Public safety communications staffs have expressed interest in redundancy in their radio systems. In order to provide redundancy, NCRnet will be able to transport public safety radio trunk communications between emergency communications centers in neighboring jurisdictions, or to regional centers. This will enable the radio system to continue operating in a jurisdiction in the event of failure of the radio system controller or loss of the emergency communications center and enable dispatchers to operate from an alternate center in the region.

In order to provide this redundancy, radio channels can be transported to any NCRnet location via native T1 circuits. The T1 circuits themselves can be redundantly routed within NCRnet, so that they continue operating even in the event of a fiber cut or loss of a facility.

For radio trunking and other applications that require native T1 circuits, 28 T1 circuits will be provisioned at each NCRnet site, 14 in each direction.

2.3.2 Telephony

Jurisdictions need voice services on NCRnet. The need is for:
1. Reliable and secure person-to-person communications and conference calls independent of the public switched telephone network, which may become overloaded in emergencies,
2. Redundancy of connections to the public switched telephone network, and
3. Reduction of public network usage for communications from jurisdiction to jurisdiction.

At present, the NCR is split between jurisdictions that are using IP-based systems for internal voice communications and those that are circuit-based (but likely considering migration to IP-based communications).

Both IP and circuit-based voice switches can be configured to connect calls to NCRnet jurisdictions via a gateway to NCRnet. The calls can travel via IP configured for guaranteed Quality of Service (QoS) or via dedicated T1 circuits.

In addition, one or more NCRnet data centers may be configured with a voice switch with connectivity to a telephone company or IP voice service provider. NCR jurisdictions may choose this as a primary or secondary means of reaching the public switched telephone network.

In order to estimate the need for voice communications on NCRnet, we assume that the equivalent of all jurisdiction trunk lines to the public switched telephone network is needed by each jurisdiction, and that those lines are routed to the data center.

2.4 Data Communications

2.4.1 WebEOC/GIS/CAD

One of the critical objectives of the NCRIP, of which the NCRnet is one component, is the availability of advanced communications between emergency operations centers and first responders. Most jurisdictions are planning to use WebEOC as the front-end interface to incident boards, messaging, video conferencing, and other operations. WebEOC is running on servers at multiple jurisdictions and is accessed on desktop and laptop computers for individual responders. The network capacity requirements for WebEOC depend on the type of usage within WebEOC. If the information is primarily text-based, individual usage will be in the tens of kbps range.

Similarly, with computer-aided dispatching (CAD), if the information transferred is primarily text-based, individual utilization of inter-jurisdictional capacity will be relatively light.

However, first responders and operations centers increasingly demand graphical geographic information, some of which may be available locally within a jurisdiction and other of which might only be available at a regional data center or at another jurisdiction. GIS maps may require tens or hundreds of megabytes. Even in an environment where GIS software is resident at each jurisdiction and maps are continuously updated on both sides, there will be the need to transport finished maps between jurisdictions in an emergency, simply because it is not possible to predict exactly what type of report or location will be needed, or where that information will reside.

In order for maps to be received or analyzed in a timely manner, inter-jurisdictional connections would therefore need to be tens or hundreds of Mbps, to facilitate simultaneous transmission of a handful of maps in less than ten seconds. The prevailing model for regional geographic information transfer calls for a metadata server to be located at a regional facility, for requests to be processed by the metadata server, and for the actual information to transfer from the source to the requester via the network. This can be modeled as outbound data from the source network and inbound data at the recipient network. If the chosen model uses an actual physical data center, it can be reworked essentially as a client-server operation from the center.

Video communications within EOC operations will also be available within WebEOC and other EOC-specific software. From the point of view of network capacity, it is already included as either operation-center or desktop video within the video category already discussed.

2.4.2 Data Recovery and Backup

The region's jurisdictions expressed interest in data recovery and backup. NCRnet will facilitate storing data in diverse locations for the purposes of recovery in the event of an outage or a disaster situation. Many of the NCR jurisdictions have data and records stored in either a single backup location within the boundaries of the jurisdiction, and/or have designated a contractor to pick up and store backup tapes.

Jurisdictions are likely to use NCRnet for backing up or recovering key or first-tier resources. Backup can be to a dedicated backup facility or via reciprocal arrangement with one or more other NCR jurisdictions.

Jurisdictions expressed a need for reliable high-speed connectivity between the backup location and their networks, some for remote management and daily backups, others for live mirroring of their networks. It will therefore be very important to connect the backup to the home networks over diverse physical routes. Adequate capacity will be needed for storage area networking (SAN) over the fiber, although some jurisdictions indicated that IP solutions would be acceptable.

Backup to a regional facility provides survivability in the event of all but the largest-scale disasters, and also enables jurisdiction staff and contractors to quickly begin work at the backup facility. However, the jurisdictions may also wish to consider backup of key information outside the Washington, DC region. NCRnet can enable jurisdictions to peer with the National LambdaRail (NLR), a not-for-profit fiber optic infrastructure, which can provide dedicated fiber optic wavelengths for high-speed connections to metropolitan areas and university campuses across the U.S. Jurisdictions can place servers and storage at a distant data center and communicate with them at full speed in real time via NLR and NCRnet.

NCRnet can support:

1. Live mirroring of data; or
2. Batch backup of data at regular intervals.

By definition, live mirroring requires network connectivity to the "mirror" site at a data rate equivalent to the aggregate rate of all simultaneous data transfers by users to the primary data resource. Real-time mirroring of data could have bursty requirements demanding extremely large amounts of bandwidth on a momentary basis. With 100 Mbps Ethernet connectivity as the norm for desktop-connected users within an enterprise or institution, the data connectivity rate to a server containing a graphics-intensive database, such as a document-imaging server or a Geographic Information System (GIS) server with dozens of potential simultaneous users, could reach a significant percentage of the server's 1 Gbps Ethernet network interface during peak usage. Extrapolating the server access rate within a government to mirroring across the region, a single set of IT recovery sessions may require one or two Gigabit interfaces across NCRnet for one or two mirrored high-performance document imaging or GIS servers.

If data backup is instead performed at regular intervals, rather than continuously, the required backup data rate depends on the amount of data to backup and the maximum acceptable length of time to perform the backup. In some cases, this may have minimal bandwidth demands if only incremental changes are copied on a daily basis.

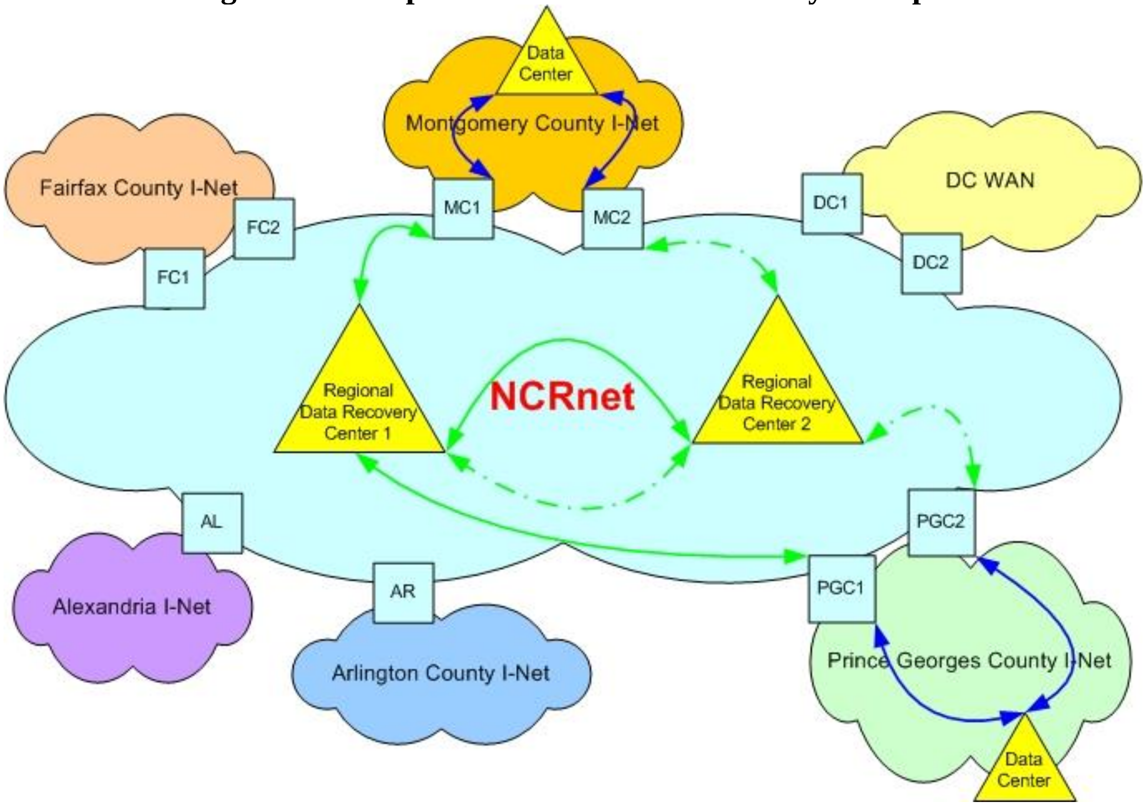
The actual amount of bandwidth required by any jurisdiction for data backup depends heavily on the type of storage and backup technique, particularly in relation to whether all protected data is re-written to the remote data facility or only incremental changes are copied.

To approximate the bandwidth requirements for NCRnet, we assume average requirements will fall somewhere between the bursty demands of continuous real-time mirroring and the part-time, high capacity loads of scheduled backups for all data. Specifically, our estimate assumes the need to perform daily backups of incremental changes for all storage on a scheduled basis, with a large percentage of all data re-written to an offsite storage center.

Based on preliminary data collected from a portion of the NCR jurisdictions, we assume a large jurisdiction may need to protect in the range of 20 TB (20,480 GB) of data, medium jurisdictions may need to protect in the range of 5 TB (5,120 GB), and small jurisdictions may need to protect some fraction of 1 TB (1,024 GB). We assume backups must be accomplished during non-typical business hours in approximately 12 hours or less, since certain backup techniques could place a demand on production storage or application servers that might otherwise interfere with normal business. This equates to the need for data rates of up to 3.8 Gbps, 970 Mbps, and 194 Mbps each for large, medium, and small jurisdictions, respectively.

Figure 2 depicts an example of centralized data recovery based on primary and backup data centers under NCRnet governance and shows example flows between the redundant regional data centers and data centers in two participating jurisdictions. Similar connections could be present for all the communities participating in NCRnet.

Figure 2: Example Centralized Data Recovery Example



2.4.3 Remote Access/Telecommuting

Particularly in the event of an emergency, the jurisdictions note their need for a means of linking remote users who are not at jurisdiction or NCRnet facilities to their networks. From home or from private Internet accounts, authorized remote users can connect to NCRnet resources or jurisdiction resources via the Internet by use of virtual private networking.

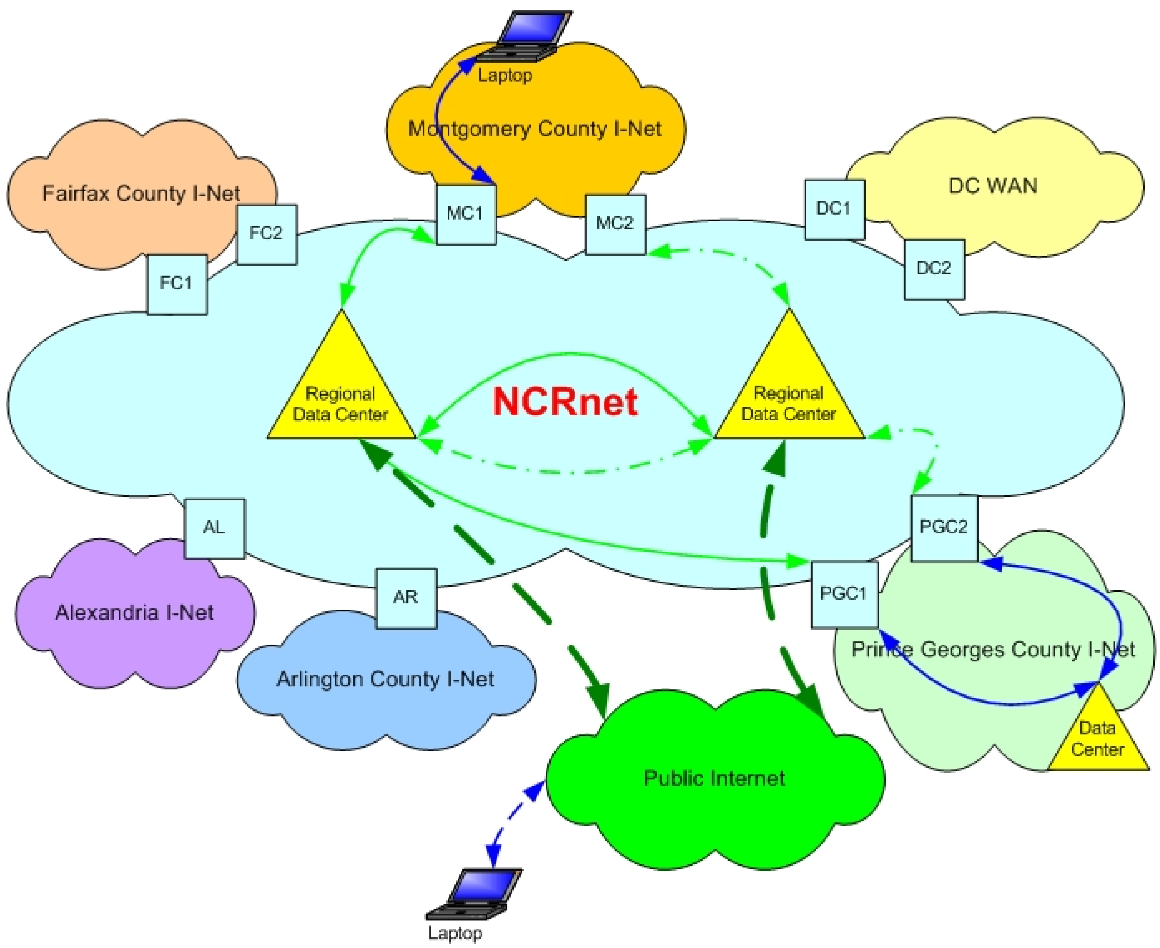
Alternately, jurisdictions may wish to enable their staff to telecommute from the government facilities of other NCR jurisdictions, for example, in the event of bad weather or a regional emergency. Jurisdictions may set aside designated telecommuting centers where other staff in NCR can perform their responsibilities, or potentially have those staff work alongside their agency counterparts in other jurisdictions.

NCRnet can enable “out-of-position” staff to work more effectively by connecting them to their home jurisdiction. As long as the staff can present appropriate credentials, a host jurisdiction could provide staff with a means to connect, such as via their own laptops or via guest accounts on desktops, to a VPN tunnel to their home jurisdiction, transported on NCRnet. The approach can be done today in the absence of NCRnet, but would require use of the host jurisdiction’s Internet capacity. Again, NCRnet provides the ability to avoid reliance on public networks, reducing costs and increasing robustness in the event of emergency.

The NCRnet capacity needed for this type of communications is included in the 50% added to the current Internet usage, which will account both for the remote access via the Internet and the internal, jurisdiction-to-jurisdiction remote access.

Figure 3 depicts two possible methods of providing remote access. Remote access could be provided for personnel connecting at participating jurisdictions (E.g., a Prince George's County user with a laptop in Montgomery County connects to Prince Georges County data center via NCRnet). The same user could also access NCRnet resources remotely through the public Internet using secure VPN technology.

Figure 3: Remote Access by Prince George's County Staff over NCRnet and Internet



2.4.4 Broadband Wireless Backhaul

NCRIP includes a broadband wireless component for access to first responders in the field and in vehicles. The broadband wireless network supports existing first responder operations, such as CAD, plus emerging graphics and video operations.

The broadband wireless architecture calls for approximately 100 antenna (base station) locations and three redundant broadband wireless network hubs. Each broadband wireless base station handles up to 13 Mbps downstream (network to user) and 4 Mbps upstream (user to network) data. At peak usage, all base stations operate at full speed, thus the peak capacity needed from the base stations to the hubs is approximately 1.3 Gbps. Since the broadband wireless network base stations will be distributed both to meet requirements for geographic coverage and capacity, the amount of the data capacity required for backhaul over NCRnet to and from each jurisdiction can be roughly approximated to correspond with the categories of participants. Specifically, we estimate small, medium, and large jurisdictions will contain on average two, five, and fifteen base stations each, respectively, corresponding to an aggregate one-way backhaul requirement of 26 Mbps, 65 Mbps, and 195 Mbps for small, medium, and large jurisdictions, respectively. This network traffic may be contained within a given jurisdiction, or travel across NCRnet for accessing resources in another jurisdiction or at a central data center.

2.4.5 Patient Tracking

One significant initial application for the NCRIP is the Patient Tracking System, in which medical first responders at a mass-casualty incident can identify patients, perform triage, and enter patient information wirelessly into the system. Medical first responders at the incident can also query the system to determine hospital availability. Patient tracking information can be made available to decision makers and authorized individuals within the medical community. The system may be integrated with RFID tags for each patient, and is designed to reduce the number of times that paramedic and hospital staffs need to determine and enter information about a patient.

The patient tracking data flow is composed of two components:

1. Mobile or field communications and
2. Communications between fixed facilities (hospitals, emergency operations centers, public health facilities, public health databases, regional decision-makers).

The field communications component and its backhaul communications is already included as part of the broadband wireless communications component estimate for NCRnet. Therefore, Table 1 includes only the communications between fixed facilities.

Information in the Patient Tracking System will be stored in one or more databases. It is assumed that the databases will be present at a data center on NCRnet. Therefore the primary usage of NCRnet will be between these databases and:

1. Wireless users via the hubs of the broadband wireless network,
2. Jurisdiction public health facilities,
3. Emergency operations centers and jurisdiction decision makers, and
4. Hospitals via the Internet and dedicated wireless links.

The capacity needed for use of the databases depends on the type of content to be accessed and stored (photos, X-rays, graphics) and the number of users that are likely to seek the data. Assuming that the larger data records only have one or two photos and no high-resolution medical images, they would be approximately 500 KB apiece. Assuming a need for access and storage of records of ten records within one second at peak times, a 40 Mbps data rate will be needed to and from the data center for this application. Some of this data will travel from the data center on and off of the Internet to reach the hospitals, clinics, and other facilities not connected to NCRnet—Table 1 estimates that one half of the data enters and leaves the data center in this manner. The remainder will be used by and posted by jurisdictions—public health staff, first responders, and operations centers. The traffic will be apportioned among the jurisdictions proportionate to the number of users on jurisdiction networks.

2.4.6 Internet Access

It is anticipated that NCRnet will connect to two or more Internet service providers for cost-effective, reliable, load-balanced service. Since NCRnet is likely to be a larger customer than any individual jurisdiction, jurisdictions can take advantage of an economy of scale in purchasing large pipes of Internet service, especially since NCRnet can be designed to connect directly to major Internet peering locations in the region.

The amount of Internet access will be estimated based on the current Internet utilization of the jurisdictions. One of the benefits of a regional Internet connectivity would be the ability to share redundant, load balancing links to increase reliability for even the smallest jurisdictions. Some larger jurisdictions are already using redundant links. For example, Arlington has two DS3 (45 Mbps) connections to the Internet. We assume on average the need for redundant T1 capacity (1.5 Mbps each, total 3 Mbps) to the Internet for small jurisdictions, redundant fractional DS3 capacity (45 Mbps total) for medium jurisdictions, and redundant DS3 connections (90 Mbps total) for large jurisdictions. It is assumed that the Internet is accessed at the data centers and distributed to and from the jurisdictions based on their current utilization levels.

In addition to supporting the existing and future needs of jurisdictions, it will be necessary to increase access to the Internet for new NCR applications. These may include access by hospitals, clinics, and physicians to patient tracking systems; coordination with first responders and decision makers outside the NCR; remote access to jurisdiction networks and NCRnet by authorized telecommuters; and access to databases outside the NCR, such as the ESSENCE public health database. Also, a significant percentage of the Internet access may be encrypted and travel via virtual private network tunnels. To account for increased usage, 50 percent will be added to the current jurisdiction usage.

It is assumed that all NCRnet jurisdictions are protected from other NCRnet users via firewalls. There will be additional firewalls between NCRnet and the Internet in order to protect NCRnet from unauthorized external access, viruses, and denial of service attacks.

2.5 Other, Non-Emergency Uses

NCRnet is designed to operate during emergency and non-emergency situations. As a result of the network's planned fiber-optic physical plant, it has high capacity and can be upgraded without construction of new cables or outside plant. For that reason, it can support applications beyond its primary first-responder mission without limiting its usefulness to the first-responder community.

2.5.1 General Government Applications

NCRnet will thus be able to support routine general-government applications, such as regional use of planning and financial information, sharing of voter rolls, and aggregation and redundancy of voice and Internet service. It can enable the jurisdictions to route all inter-jurisdictional communications such as emails and telephone calls through private channels, reducing expenditures for data and voice services.

2.5.2 Educational Applications

As most jurisdiction networks in the region connect educational as well as government facilities, NCRnet will be able to regionally interconnect school districts, community colleges, and area higher learning institutions, facilitating distance learning, mentorship, field trips, and in-service training. Connectivity of schools with NCRnet will also have a direct first responder benefit because the schools may serve as emergency shelters, and it may be critical to communicate with schools in certain types of regional emergency.

2.5.3 Connectivity to National and Global Networks

A high-speed, reliable NCRnet may also leverage the capabilities of existing national and global networks that have connection points in the NCR. For example, the Mid-Atlantic Crossroads (MAX) network is present at points in the region and is connected to the National LambdaRail network, a national network that provides its users with dedicated fiber optic wavelengths throughout the U.S. By connecting NCRnet to these networks, NCRnet participants may be able to receive high-speed Internet service at low cost and access to Internet2. These networks may also enable NCRnet jurisdictions to establish data recovery and backup centers at cities across the U.S.

3 Comparison Between a Leased Network and One Owned by the NCR

Leasing circuits eliminate the need for the jurisdiction to own and operate a data network. It also avoids the addition or management of contract staff to operate and maintain the network. In addition the upfront cost of circuit leasing is lower than constructing private fiber, and the time to deployment is often less when working with leased circuits. Leasing, however, has critical disadvantages that make it much less desirable for emergency support services. Specifically:

- Leased services do not offer total control and management over a communications link
- The availability of a leased circuit may not be accurately assessed due to the lack of knowledge of a leased provider's proprietary network and its physical infrastructure
- Leased services are not independent of the network's used by the public
- Network security is the responsibility of the provider between end points

3.1 Control and Management of Leased Services

A network built upon leased network services obtained from a service provider cannot provide the control and management that is available in a privately owned and operated network.

Leased network services are in essence a "black box" in terms of control and management. The leased provider is relied on to maintain and operate the core equipment of a leased service. This entails configuring the equipment, monitoring the hardware and physical infrastructure, and performing routine maintenance.

NCR's inter-jurisdictional capacity requirements include; video, voice and data communications. Both voice and video services usually require dedicated bandwidth. Two way voice and video services require dedicated bandwidth and very predictable transmission delay properties.

In other words, linking two-way radio communications systems or supporting videoconferencing over IP or using TDM connections requires the ability to manage bandwidth across the entire network. Although this functionality can be provisioned on the edge device when using a managed service provider for connectivity, owing a private fiber network will give NCRnet control and the ability to increase bandwidth based on NCRIP's time frame (which will in turn allow NCRIP to properly plan for integration of new applications without an increase in cost for provision new bandwidth). Furthermore, it offers the ability to implement advanced QoS mechanisms that are enforced on a network-wide, end-to-end basis.

To make changes in the core of the network for a new application, increase bandwidth, or to implement new policies for enhanced QoS, the lessee must request that the provider make configuration changes to the network, oftentimes at the expense of the lessee.

The lessee is also not able to control who manages and maintains the core of the network. The knowledge, skill set, and security background of those operating the network is often beyond the control of a lessee.

With a private fiber optic network, each piece of the communications network is controlled and managed by the owner. The owner may choose to operate the network on its own with its own staff, or it may outsource the operations to a contractor of its choosing. Either way, choices regarding the management of the network are in the hands of the owner.

3.2 Availability of Leased Services

The availability of a communications link is derived from the probability of a failure within the network between two points. In a leased circuit network, the end user is not aware of all of the potential risks to availability of the network. Several key factors that affect availability and cannot be determined by a lessee include:

- Physical redundancy in the plant;
- Physical redundancy in the building entrances;
- Physical redundancy in the networking equipment;
- Ensuring network equipment is properly configured and regularly tested to take advantage of hardware and link redundancy;
- Redundancy for power and HVAC;
- How many facilities the circuit crosses between endpoints;
- Whether the plant is located underground or aerial;
- Who has access to the core networking equipment and plant;
- How old or well maintained the core equipment is;
- How the system is monitored and maintained; and
- What are the single points of failure in the communications link.

Many of the factors can be approximated or relative numbers may be obtained from the leased circuit provider; however for critical government services such as public safety, the approximations and availability estimates from leased network services may not meet the availability requirements of a critical traffic network. In the case of physical architecture issues, such as the physical routes of cabling, approximations are not sufficient, and detailed maps are usually considered proprietary and confidential to a commercial provider.

In addition, lessees are subject to the providers schedule for repair and maintenance of the circuit. Although it may be possible to include provisions in the service level agreement (SLA) for special priority service restoration, it is unlikely that SLAs will be adhered to during major disaster events. Furthermore there may be no way to ensure that a leased circuit for public safety is the first link to be repaired during a major disaster.

A similar problem can arise in both scheduled and unscheduled maintenance of a leased circuit. The timing of these maintenance downtimes may not correspond to available downtimes in a public safety network. In a private network such as NCR, maintenance downtimes can be coordinated to the extent they are scheduled to minimize downtime and change operational procedures to prepare for a network outage,

SLAs often guarantee availability and repair time, but typically do not hold true for a major disaster. Furthermore service providers usually rely on cash rebates to handle outages to the network, although cash rebates may not be a suitable alternative to outages on a public safety network.

3.3 Independence from Public Communications Networks

A privately owned communications network does not rely on physical infrastructure, equipment, or other resources that also carry public traffic for residents and businesses. Shared resources are used by a managed network service provider to reduce their cost by taking advantage of the statistical nature of communications traffic. In other words, commercial carriers intentionally oversubscribe their networks to minimize costs (maximize profits), since all of their customers are not likely (statistically speaking) to simultaneously use their services to full capacity all of the time. The advantage of an independent network is that increases in public traffic on the network or public network outages do not affect privately owned networks.

Additionally, the only way to ensure that there is adequate bandwidth is to overbuild a network to support maximum capacity demand, not average utilization (while absorbing the cost even if the bandwidth is not used). Some leased managed services offer the ability to be charged only for the bandwidth that is used however, capacity is limited. Typically, these services are only effective in saving cost when institutions have a specific understanding of their applications' bandwidth requirements. NCRnet, which is designed to support regional initiatives and interoperate with existing jurisdictions' network infrastructures, can provide a more reliable, higher capacity, flexible network infrastructure by owning a private infrastructure.

As is the case in many major public safety incidents, public networks, such as the Public Switched Telephone Network (PSTN) and the Internet are often overloaded by the amount of traffic on the network. This can lead to busy signals on the PSTN and a lack of connectivity on the Internet. Privately owned networks typically do not experience the same traffic increases and can be designed to handle any expected traffic increase during a major incident.

Many public networks are in the planning and early implementation stages of providing priority and preemption capabilities for most managed service providers and will not be universally available, however in the event of a crisis, priority and preemption is critical for public safety networks.

A privately owned NCRnet can prioritize bandwidth both in the core and at the edge. This will allow NCR the capability of prioritizing by location and also having the capability to preempt all traffic other than public safety traffic, if necessary. More importantly, the private infrastructure of NCRnet can be allocated so certain sensitive traffic is always on dedicated capacity, since capacity can be readily scaled as needed for other applications.

3.4 Network Security

Implementation of network security on a leased circuit typically occurs at the edge of the network. Many leased networks use end-to-end encryption to securely transmit data over networks that share a core network with public users. Oftentimes the provider of a leased circuit may dictate what types of end-to-end security are allowed on a leased circuit (IP managed services for example).

In a privately owned network such as NCRnet, NCRIP is capable of offering end-to-end security throughout the network infrastructure. NCRIP will have the capability to offer layered security which enables NCRnet to be robust and highly secure.

In addition to data security, a privately owned network allows the owner to manage physical security as well as network security. This includes:

- Access to facilities and networking rooms
- Passwords to edge equipment and firewalls
- Network access and authentication
- Monitoring of networking rooms, including security alarms, surveillance cameras, etc.
- Desktop security
- Equipment placement and provisioning

4 Cost Comparison Between Leased and Owned Networks

Up to this point, this document has focused on projecting the capacity demands of potential communications applications for NCRnet; and demonstrating the functional advantages of a privately owned network infrastructure. The functional demands of public safety applications alone seem to indicate that leased services should not even be considered a viable, regardless of cost. However, it can also be shown that a private infrastructure is the most cost-effective approach for NCRnet in the long-run.

Comparing the cost between a leased service and a privately owned and operated network is not trivial, as it requires making certain assumptions regarding future requirements and/or future costs of leased services. Fortunately, private infrastructure costs, including both hardware and physical cable plant, remain relatively constant with respect to initial and ongoing expenses (though their capabilities increase with time).

The only uncertainty that must be addressed is how long is the "long-run" with respect to recouping the initial capital investment for private infrastructure. Towards this end, we compare the costs of private network infrastructure to leased services based on two opposite extreme models to demonstrate the possible range of cost recovery scenarios:

1. Model 1 - Providing equivalent initial capacity for all links with both types of networks (private vs. leased), assuming the projected (high-end) capacity requirements for each

2. Model 2 – Providing high capacity links using private infrastructure versus using leased services to meet only the very minimal requirements of existing or imminent regional application deployments

Obviously, Model 2 will indicate a longer time to recoup expenses for private infrastructure relative to leased services when compared to Model 1, but presents the most conservative illustration with respect to NCRnet demand projections for demonstrating the cost-effectiveness of private infrastructure. In other words, even if NCRnet only ever supports a minimal level of applications and services, it can still be shown that it is more cost effective when built using private infrastructure. Moreover, the tremendous capacity afforded by the private infrastructure will help ensure that its stakeholders will demand much more than the minimal array of service from it.

4.1 Cost Comparison Model 1

For Model 1, we examine an "apples-to-apples" comparison of leased services to a privately constructed NCRnet with respect to the capacity provided by each. Furthermore, we assume the need to support the full array of applications discussed previously in this document.

In Table 3, the required capacity and year required are listed. As can be seen, the capacity requirements are substantial relative to typical leased service offerings.

Table 3: Estimated NCRnet Capacity Requirements Summary (Per Jurisdiction)

Link		Phase	Year	Capacity (Mbps)
Montgomery County	Fairfax County	I	1	155
Montgomery County	District of Columbia	I	1	155
Montgomery County	District of Columbia	I	1	2,500
District of Columbia	Arlington County	I	1	155
District of Columbia	State of Maryland (Oxon Hill Tower)	I	1	155
Prince George's County	State of Maryland (Oxon Hill Tower via District Heights Tower)	I	1	155
Fairfax County	Prince William County	I	1	155
Fairfax County	State of Maryland (Oxon Hill Tower)	I	1	155
Arlington County	Fairfax County	I	1	2,500
Arlington County	Alexandria	I	Existing	1,000
District of Columbia	Prince George's County	II	2	2,500
District of Columbia	Prince George's County (redundant)	II	2	2,500
Montgomery County	Fairfax County	II	2	10,000
Fairfax County	Arlington County	II	2	10,000
Arlington County	District of Columbia	II	2	10,000
District of Columbia	Council of Governments	II	2	10,000
District of Columbia	Council of Governments (redundant)	II	2	10,000
Montgomery County	District of Columbia	II	2	10,000
Arlington County	Alexandria	II	2	2,500
Alexandria	Fairfax County	II	2	2,500
Prince William County	Fairfax County	III	3	2,500
Prince William County	Fairfax County (redundant)	III	3	2,500
Fairfax County	Loudoun County	IV	4	2,500
Loudoun County	Prince William County	IV	4	2,500
Frederick County	Montgomery County	IV	4	2,500
Frederick County	Loudoun County	IV	4	2,500

To estimate the lease costs to support these requirements, we used Sprint's GSA rate for dedicated IP service cost. In addition, we estimated the required non-recurring charges for equipment and activation. It is quite likely that Sprint or other carrier may have additional non-recurring charges to connect to a given location. The estimate lease costs are shown in Table 4.

Table 4: Estimated Leased Network Costs

Link		Phase	Year	NR Costs	Annual Lease Cost
Montgomery County	Fairfax County	I	1	$ 6,000	$ 634,764
Montgomery County	District of Columbia	I	1	$ 6,000	$ 634,764
Montgomery County	District of Columbia	I	1	$ 24,000	$ 1,450,884
District of Columbia	Arlington County	I	1	$ 6,000	$ 634,764
District of Columbia	State of Maryland (Oxon Hill Tower)	I	1	$ 6,000	$ 634,764
Prince George's County	State of Maryland (Oxon Hill Tower via District Heights Tower)	I	1	$ 6,000	$ 634,764
Fairfax County	Prince William County	I	1	$ 6,000	$ 634,764
Fairfax County	State of Maryland (Oxon Hill Tower)	I	1	$ 6,000	$ 634,764
Arlington County	Fairfax County	I	1	$ 24,000	$ 1,450,884
Arlington County	Alexandria	I	Existing	$ 18,000	$ 808,140
District of Columbia	Prince George's County	II	2	$ 48,000	$ 2,901,768
District of Columbia	Prince George's County (redundant)	II	2	$ 48,000	$ 2,901,768
Montgomery County	Fairfax County	II	2	$ 192,000	$ 11,607,072
Fairfax County	Arlington County	II	2	$ 192,000	$ 11,607,072
Arlington County	District of Columbia	II	2	$ 192,000	$ 11,607,072
District of Columbia	Council of Governments	II	2	$ 192,000	$ 11,607,072
District of Columbia	Council of Governments (redundant)	II	2	$ 192,000	$ 11,607,072
Montgomery County	District of Columbia	II	2	$ 192,000	$ 11,607,072
Arlington County	Alexandria	II	2	$ 48,000	$ 2,901,768
Alexandria	Fairfax County	II	2	$ 48,000	$ 2,901,768
Prince William County	Fairfax County	III	3	$ 48,000	$ 2,901,768
Prince William County	Fairfax County (redundant)	III	3	$ 48,000	$ 2,901,768
Fairfax County	Loudoun County	IV	4	$ 48,000	$ 2,901,768
Loudoun County	Prince William County	IV	4	$ 48,000	$ 2,901,768
Frederick County	Montgomery County	IV	4	$ 48,000	$ 2,901,768
Frederick County	Loudoun County	IV	4	$ 48,000	$ 2,901,768

The estimated build costs for a private NCRnet, including annual operation and maintenance costs, are shown in Table 5.

Table 5: Estimated Build Costs

Link		Phase	Year	Implementation Costs	Annual Operating & Maintenace Costs
Montgomery County	Fairfax County	I	1	$ 270,000	$ 13,500
Montgomery County	District of Columbia	I	1	$ 270,000	$ 13,500
Montgomery County	District of Columbia	I	1	$ 250,000	$ 12,500
District of Columbia	Arlington County	I	1	$ 270,000	$ 13,500
District of Columbia	State of Maryland (Oxon Hill Tower)	I	1	$ 270,000	$ 13,500
Prince George's County	State of Maryland (Oxon Hill Tower via District Heights Tower)	I	1	$ 270,000	$ 13,500
Fairfax County	Prince William County	I	1	$ 270,000	$ 13,500
Fairfax County	State of Maryland (Oxon Hill Tower)	I	1	$ 270,000	$ 13,500
Arlington County	Fairfax County	I	1	$ 250,000	$ 37,500
Arlington County	Alexandria	I	Existing	$ -	$ -
District of Columbia	Prince George's County	II	2	$ 400,000	$ 60,000
District of Columbia	Prince George's County (redundant)	II	2	$ 400,000	$ 60,000
Montgomery County	Fairfax County	II	2	$ 500,000	$ 75,000
Fairfax County	Arlington County	II	2	$ 80,000	$ 12,000
Arlington County	District of Columbia	II	2	$ 80,000	$ 12,000
District of Columbia	Council of Governments	II	2	$ 250,000	$ 37,500
District of Columbia	Council of Governments (redundant)	II	2	$ 200,000	$ 30,000
Montgomery County	District of Columbia	II	2	$ 80,000	$ 12,000
Arlington County	Alexandria	II	2	$ 80,000	$ 12,000
Alexandria	Fairfax County	II	2	$ 650,000	$ 97,500
Prince William County	Fairfax County	III	3	$ 400,000	$ 60,000
Prince William County	Fairfax County (redundant)	III	3	$ 600,000	$ 90,000
Fairfax County	Loudoun County	IV	4	$ 400,000	$ 60,000
Loudoun County	Prince William County	IV	4	$ 600,000	$ 90,000
Frederick County	Montgomery County	IV	4	$ 400,000	$ 60,000
Frederick County	Loudoun County	IV	4	$ 700,000	$ 105,000

As seen in Table 4 and Table 5, the build option has lower implementation costs and operating costs. The comparison of all costs for each option for Years 1 through 4 is shown in Table 6.

Table 6: Model 1 Lease versus Build Cost Comparison by Year

Year	Lease Cost ($000)	Build Cost ($000)
1	$ 8,261	$ 2,535
2	$ 90,747	$ 3,273
3	$ 95,302	$ 1,703
4	$ 107,005	$ 3,118

Using a net present value analysis, in the first five years[2] the lease option will cost $323 million more than the build option. Even if you assume all build costs in Year 1, the two solutions are only roughly equivalent in cost for one year. Beyond this, leased services clearly are cost prohibitive if you assume the need to support full array of application requirements discussed in this document.

4.2 Cost Comparison Model 2

For Model 2, we compare the cost of leased services to a privately constructed NCRnet assuming a much more conservative subset of the application requirements. This differs from Model 1 by requiring far less expensive leased services, offering significantly less capacity. For a privately constructed NCRnet, we continue to assume the provisioning of high capacity links, but do not include all of the link redundancy afforded by Model 1 since a leased solution from a single provider also would not provide this degree of redundancy. This model represents a “worst-case” scenario with respect to the utilization of NCRnet, and presents a much more challenging scenario with respect to recouping capital construction expenditures for a privately built network.

In Table 7, the reduced capacity assumptions are listed. These are based on only existing or imminent application deployments, limited to providing backhaul for the NCRIP Regional Wireless Broadband Network, the NCR ESF-5a Video and Audio Conferencing Solution, and the trunking of telephone services (as previously discussed).

[2] Using a six percent discount rate.

Table 7: Estimated Conservative NCRnet Capacity Requirements Summary (Per Jurisdiction)

	Link		Phase	Year	Capacity (Mbps)
1	Montgomery County	District of Columbia	I	1	2500
2	Arlington County	Fairfax County	I	1	2500
13	Montgomery County	Rockville	I	1	1000
4	District of Columbia	Prince George's County	II	2	2500
5	Fairfax County	Arlington County	II	2	10000
6	Arlington County	District of Columbia	II	2	10000
7	District of Columbia	Council of Governments	II	2	10000
8	Montgomery County	District of Columbia	II	2	10000
9	Arlington County	Alexandria	II	2	2500
14	Montgomery County	Gaithersburg	II	2	1000
15	Montgomery County	Takoma Park	II	2	1000
18	Fairfax County	City of Fairfax	II	2	1000
19	Fairfax County	Falls Church	II	2	1000
10	Prince William County	Fairfax County	III	3	2500
20	Prince George's Count	Bowie	III	3	1000
21	Prince George's Count	College Park	III	3	1000
22	Prince George's Count	Greenbelt	III	3	1000
11	Fairfax County	Loudoun County	IV	4	2500
12	Frederick County	Montgomery County	IV	4	2500
16	Prince William County	Manassas	IV	4	1000
17	Prince William County	Manassas Park	IV	4	1000
3	Arlington County	Alexandria	I	Existing	1000

Table 8 provides the corresponding lease costs to provision the capacity indicated in Table 7 for this model.

Table 8: Estimated Leased Network Costs

	Link	NR Costs	Annual Lease Cost
1	Montgomery County	$1,300	$48,000
2	District of Columbia	$1,300	$48,000
3	Prince George's County	$1,300	$48,000
4	Fairfax County	$1,300	$48,000
5	Arlington County	$1,300	$48,000
6	Prince William County	$1,300	$48,000
7	Alexandria	$1,300	$48,000
8	Loudoun County	$1,300	$48,000
9	Frederick County	$1,300	$48,000
10	City of Fairfax	$1,300	$30,000
11	Bowie	$1,300	$30,000
12	Takoma Park	$1,300	$30,000
13	College Park	$1,300	$30,000
14	Gaithersburg	$1,300	$30,000
15	Rockville	$1,300	$30,000
16	Falls Church	$1,300	$30,000
17	Manassas	$1,300	$30,000
18	Manassas Park	$1,300	$30,000
19	Greenbelt	$1,300	$30,000
20	COG	$1,300	$30,000

Table 9 provides the corresponding build costs to construct NCRnet, not including redundant links that would not be incorporated by a strictly leased solution.

Table 9: Estimated Build Costs (Without Redundancy)

	Link		Phase	Year	Implementation Costs	Annual Operating & Maintenace Costs
1	Montgomery County	District of Columbia	I	1	$250,000	$37,500
2	Arlington County	Fairfax County	I	1	$250,000	$37,500
13	Montgomery County	Rockville	I	1	$30,000	$4,500
4	District of Columbia	Prince George's County	II	2	$400,000	$60,000
5	Fairfax County	Arlington County	II	2	$80,000	$12,000
6	Arlington County	District of Columbia	II	2	$80,000	$12,000
7	District of Columbia	Council of Governments	II	2	$250,000	$37,500
8	Montgomery County	District of Columbia	II	2	$80,000	$12,000
9	Arlington County	Alexandria	II	2	$80,000	$12,000
14	Montgomery County	Gaithersburg	II	2	$30,000	$4,500
15	Montgomery County	Takoma Park	II	2	$30,000	$4,500
18	Fairfax County	City of Fairfax	II	2	$30,000	$4,500
19	Fairfax County	Falls Church	II	2	$30,000	$4,500
10	Prince William County	Fairfax County	III	3	$400,000	$60,000
20	Prince George's County	Bowie	III	3	$30,000	$4,500
21	Prince George's County	College Park	III	3	$30,000	$4,500
22	Prince George's County	Greenbelt	III	3	$30,000	$4,500
11	Fairfax County	Loudoun County	IV	4	$400,000	$60,000
12	Frederick County	Montgomery County	IV	4	$400,000	$60,000
16	Prince William County	Manassas	IV	4	$30,000	$4,500
17	Prince William County	Manassas Park	IV	4	$30,000	$4,500
3	Arlington County	Alexandria	I	Existing	$0	$0

Table 10 provides a summary comparison of the lease and build options for Model 2.

Table 10: Model 2 Lease versus Build Cost Comparison by Year

Year	Lease Cost	Build Cost
1	$ 788,000	$ 609,500
2	$ 762,000	$ 1,333,000
3	$ 762,000	$ 806,500
4	$ 762,000	$ 1,305,500
5	$ 762,000	$ 445,500
6	$ 762,000	$ 445,500
7	$ 762,000	$ 445,500
8	$ 762,000	$ 445,500
Total	$ 6,122,000	$ 5,836,500

As can be seen in Table 10, after only eight years, the privately built network offers a lower total cost with ongoing costs substantially lower than leased services on an annual basis. Moreover, the privately built network offers higher capacity, the ability to scale for more applications, and most of the functional advantages of a private infrastructure from Year 1.

4.3 Summary of Cost Analysis

Two extreme cost comparison models were examined in this document, both of which demonstrate that leased services offer less functionality and higher overall costs relative to constructing a private fiber optic network offering far greater functional advantages.

In the first model, if we assume that NCRnet is to meet the full range of application requirements for which it is intended, leased services become so expensive that even a year of leased services becomes more expensive than constructing a private network.

In the second model, we assume a much less ambitious undertaking of supporting only those applications that are already being deployed or currently in used by the jurisdictions. Although this reduces the capacity requirements and associated leased costs to a level that is more palatable, the cost of a private fiber network would be recouped in just eight years relative to the leased services. Meanwhile, with the build option, a much higher capacity network is achieved from Year 1, operational costs from Year 8 are more than $300,000 less than the leased solution, and the scalability to support more applications without directly increasing operational costs exists (due to the scalable nature of fiber optics).