Department of Homeland Security

Pandemic Influenza Impact on Communications Networks Study

December 2007

UNCLASSIFIED

Homeland Security

Executive Summary

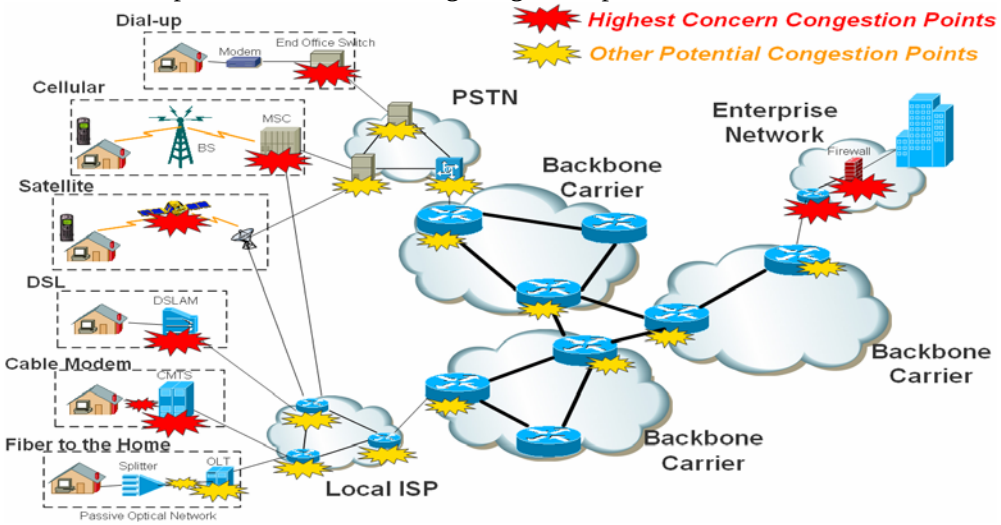
There is widespread concern among policymakers and public health experts about the possibility of a worldwide pandemic outbreak. In preparation for dealing with a pandemic scenario in the United States, several national plans have been released by the Homeland Security Council (HSC), Department of Homeland Security (DHS), Department of Health and Human Services (HHS), and other organizations. Many of these national plans identify telecommuting as a key component of the national response to a pandemic influenza. Despite increasing adoption of telecommuting as a normal method of business, the technical feasibility of widespread telecommuting given the existing infrastructure is not well established. In particular, businesses may not be prepared to handle the surge in telecommuting traffic and telecommuters may face congestion when competing for network resources due to an increase in recreational users and children home from school.

The Pandemic Influenza Impact on Communications Networks Study was undertaken to address the following questions:

- *Will the telecommuting strategy succeed during a pandemic influenza?*
- *What preparations can be done to better prepare for telecommuting during a pandemic influenza?*

This study was coordinated under the DHS Office of Cyber Security & Communications (CS&C), which is the sector specific agency for Information Technology and Telecommunications as designated by the DHS *National Infrastructure Protection Plan – 2006*. Industry and government collaboration was critical to the study. Subject matter experts in industry and government in the fields of communications, information technology (IT), cyber security, epidemiology, business continuity planning, financial services, and emergency response have supported the study.

The methodology for the study included three major areas: Identification of Potential Congestion Points, Recommended Preparations, and Modeling. Identification of Potential Congestion Points involved examining the communications infrastructure and the anticipated change in network user behavior to identify potential congestion points for telecommuting during a pandemic scenario. Consensus was reached that the general areas of highest risk for congestion from the perspective of telecommuting are enterprise networks and residential Internet access networks. Enterprise network configurations vary widely across organizations and many may not be sized to accommodate the anticipated increase in telecommuting traffic during a pandemic. Residential Internet access networks may face localized congestion due to increased traffic loads above normal peak usage. The figure below identifies potential telecommuting congestion points.



In order to address the potential congestion points, phased preparations are proposed for the pandemic scenario. In the short term, communications and IT best practices have been identified that can better prepare the telecommuting strategy to succeed. The best practices address only communications and IT issues and should be taken in the context of larger pandemic planning efforts. The best practices were developed through industry and government consensus and may need to be tailored to specific local circumstances. The communications and IT best practices are separated into four categories:

- **Enterprise Network Best Practices** – Guidance for businesses and government organizations on preparing enterprise IT infrastructures to support an anticipated increase in telecommuting traffic during a pandemic
- **Telecommuter Best Practices** – Guidance for business and government telecommuters on techniques to maintain business continuity while working from residential access networks
- **General Public Best Practices** – Guidance for the general public on voluntary actions to help reduce potential congestion in residential access networks
- **Network Service Provider Best Practices** – Guidance for network service providers on maintaining operations and existing service levels during a pandemic

In the long term, Next Generation Network (NGN) Priority Services could potentially support business continuity during a pandemic by providing priority to critical telecommuter groups, if the required features are designed into the commercial communications infrastructure. Current priority communications services include Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP). The DHS National Communications System (NCS) is working with the communications industry to migrate GETS and WPS into NGN architectures, as well as provide new priority services such as priority Internet access, video teleconferencing, and email. Initial capabilities of these services are not expected to be available until 2011-2012.

A model was developed to analyze the relationship between a pandemic spread, network user behavior, and network performance. The model was used to quantify the impact of a pandemic on the communications infrastructure and assess the potential effect of communications and IT best practices on improving telecommuting performance. Some key findings from the model include:

- **Pandemic Parameters** – Pandemic disease parameters can significantly change the peak network user population.
- **Best Practices** – In many pandemic scenarios, a high rate of compliance with all communications and IT best practices can enable the telecommuting strategy to succeed. In particular, limiting video traffic appears to have a large impact.
- **Worst Case** – Potential pandemic scenarios exist that indicate a high risk for Internet congestion. These include high absenteeism pandemic scenarios (i.e. large home network user population) and low compliance with the communications and IT best practices.

Will the telecommuting strategy succeed during a pandemic influenza?

The unique features of a pandemic outbreak in the U.S. cannot be accurately predicted in advance. The specific pandemic parameters, quarantine decisions, and human behavior may not be realized until an actual pandemic. From the telecommuting perspective, the most important parameter is the absenteeism level that causes the change in home network user population. For the existing commercial communications infrastructure without any additional preparations, it is concluded that:

- In a low absenteeism pandemic scenario, the telecommuting strategy is anticipated to be successful for the majority of telecommuters.

- In a 40 percent absenteeism scenario, the telecommuting strategy is expected to be significantly impacted for most telecommuters during the peak of the pandemic.
- In a high absenteeism scenario, the telecommuting strategy is expected to be unusable for the majority of telecommuters during the peak of the pandemic.

What preparations can be done to better prepare for telecommuting during a pandemic influenza?
In the short term, communications and IT best practices have been identified that can better prepare the telecommuting strategy to succeed. Key takeaways from the best practices include:

- **Enterprise Networks** – Businesses should use 40 percent as a guideline, but should assess their particular telecommuting needs for a pandemic situation and size their remote user capabilities appropriately.
- **Telecommuters** – Employees who plan to telecommute during a pandemic and are truly critical to business operations should not rely on best effort, residential Internet access.
- **General Public** – Limiting non-critical recreational traffic, particularly during day time work hours, will be key to enabling the pandemic telecommuting strategy to succeed.
- **Network Service Providers** – Network service providers will also be affected by the spread of a pandemic and will be operating with a reduced workforce. This will likely limit their ability to respond to any surge in traffic and provision new capacity.

Modeling results suggest that potential pandemic scenarios exist in which the severity of the pandemic and/or low level of compliance with communications and IT best practices may still lead to network congestion. The Federal government should continue to work with industry to investigate mechanisms that could be implemented when voluntary compliance with best practices is not enough to enable the telecommuting strategy to succeed.

In order to better prepare for telecommuting during a pandemic influenza, the following actions are recommended:

- **Education and Outreach** – Identify outreach strategies to educate the government, industry, and general public on the communications and IT best practices. Compliance with the best practices may significantly improve the probability of the telecommuting strategy succeeding during a pandemic.
- **Worst Case Mechanisms** – Continue to work with industry to investigate mechanisms to implement when voluntary compliance with best practices is not enough to enable the telecommuting strategy to succeed.

Table of Contents

List of Figures

1 Introduction

1.1 Purpose

The purpose of this report is to document analysis and recommendations from the Department of Homeland Security (DHS) Pandemic Influenza Impact on Communications Networks Study. This study was coordinated under the DHS Office of Cyber Security & Communications (CS&C) which is the sector specific agency for Information Technology and Telecommunications as designated by the DHS *National Infrastructure Protection Plan – 2006*.

The President's *National Strategy For The Physical Protection of Critical Infrastructures and Key Assets – February 2003* identifies national goals and objectives that underpin efforts to secure the infrastructures and assets vital to our national security, governance, public health and safety, economy, and public confidence.

Under this strategy, DHS is directed to:

- Build partnerships with state and local governments and the private sector by designing and implementing its own processes to be open, inclusive, and results-oriented.
- Actively develop opportunities to build upon proven models.
- Identify and share the Federal government's core competencies, capabilities, and selected resources to enhance the efforts of its partners.
- Facilitate honest brokering and communication between organizations and sectors.

The DHS Pandemic Influenza Impact on Communications Network Study supports these responsibilities through joint industry and government cooperation to evaluate the potential impact on the communications infrastructure in the event of a pandemic influenza in the United States. The study examines potential communications and information technology (IT) issues during a pandemic and identifies industry and government recommendations on how to better prepare the nation to handle these challenges.

1.2 Background

1.2.1 Pandemic Influenza

A pandemic is a global disease outbreak. A pandemic influenza occurs when a new influenza virus emerges for which there is little or no immunity in the human population, begins to cause serious illness, and then spreads easily person-to-person worldwide [1]. There is widespread concern among policymakers and public health experts about the possibility of a worldwide pandemic outbreak. Pandemics are a recurring phenomenon with three pandemics occurring in the 20th century. Today, scientists are particularly worried about the H5N1 virus, a strain that has spread through bird populations across Asia, Africa, and Europe. Pandemics cannot be accurately predicted and can occur at any time of the year. Health and Human Services Secretary Michael Leavitt warned that "when it comes to a pandemic, we are over-due and underprepared" [2]. In addition to direct medical consequences, a pandemic is expected to have impacts across the economy. Travel restrictions and quarantines in response to a pandemic will limit mobility and could disrupt supply chains around the world potentially leading to a drop of close to 5 percent of Gross Domestic Product (GDP) in the United States [3].

1.2.2 Telecommuting

Several national pandemic plans identify telecommuting as a key component of the national response to a pandemic influenza [4]. Telecommuting is recommended as a social distancing enabler that can

limit disease spread, while allowing businesses to continue to function. During the severe Spanish pandemic of 1918, cities such as St. Louis, Milwaukee, and Kansas City that implemented early and aggressive social distancing measures were able to reduce disease transmission rates by up to 30-50 percent [5].

The Pandemic Severity Index, defined by Center for Disease Control (CDC), categorizes a pandemic scenario based on the case fatality ratio. The Pandemic Severity Index advises businesses to consider following telecommuting programs for Category 2 and 3 pandemics and recommends telecommuting programs as an important component of the planning strategy for Category 4 and 5 pandemics [6]. More specifically, the Homeland Security Council (HSC) has advised businesses to plan for up to 40 percent of their employees to be absent during the two week peak of a 6-8 week pandemic wave [7]. Enabling the pandemic telecommuting strategy to succeed will be key in mitigating disease spread while enabling businesses to continue operations and limiting additional impact to the economy.

1.3 Problem Definition

Given the telecommuting strategy advocated in several national pandemic plans, the following questions remain:

- *Will the telecommuting strategy succeed during a pandemic influenza?*
- *What preparations can be done to better prepare for telecommuting during a pandemic influenza?*

Spurred in part by the increasing adoption of broadband Internet access, telecommuting is a growing trend particularly in the services sector of the economy. A survey from 2006 found that approximately 8 percent of US workers have an employer that allows them to telecommute full-time and roughly 20 percent of the workforce engages in telecommuting at least once a month [8]. ***Despite the growing telecommuting trend, the feasibility of widespread telecommuting during a pandemic scenario given the existing communications infrastructure has not been established.***

Two areas of particular concern are the ability of enterprise networks and residential Internet access networks to handle increased telecommuting traffic. Many businesses with limited reliance on telecommuting today may not be capable of handling the anticipated increase in telecommuting traffic during a pandemic. Additionally, telecommuters may face congestion on residential Internet access networks. A surge in traffic on residential Internet access networks from users who are home due to illness or part of the "worried well" (those who are not sick but stay home to avoid contracting the disease) may affect the performance of workers attempting to telecommute.

A recent tabletop style simulation of a pandemic scenario conducted by the World Economic Forum judged that "the telecommunications infrastructure will be severely strained" during a pandemic [9]. In light of predictions such as these, this study was undertaken to address the questions listed above and more thoroughly analyze the potential impact on the communications infrastructure in the event of a pandemic influenza in the United States. The study also identifies steps that can be taken to better prepare the nation to support the pandemic telecommuting strategy advocated in several national plans.

1.4 Scope

This study is focused on potential impacts to the nation's commercial communications and IT infrastructure, particularly related to telecommuting. Recommendations from this study only relate to communications and IT issues and should be taken in the context of overall national pandemic planning guidance. This study assumes the general pandemic telecommuting strategy advocated in

several national pandemic plans as given [4]. The focus of the study is on examining the technical feasibility of the pandemic telecommuting strategy and identifying steps to better prepare the nation to support the strategy.

1.5 Document Organization

Section 1: Introduction – Contains material on the purpose, background, problem definition, and scope of the Pandemic Influenza Impact on Communications Networks Study

Section 2: Stakeholder Involvement – Describes industry and government involvement in the Pandemic Influenza Impact on Communications Networks Study

Section 3: Methodology – Describes the approach followed in the Pandemic Influenza Impact on Communications Networks Study

Section 4: Potential Congestion Points – Identifies potential congestion points for telecommuting during a pandemic scenario

Section 5: Recommended Preparations – Outlines a phased approach for implementing preparations to better support the telecommuting strategy during a pandemic

Section 6: Outstanding Issues – Identifies communications and IT issues either outside the scope or not fully addressed by this study

Section 7: Modeling – Provides an overview of a modeling capability developed for the Pandemic Influenza Impact on Communications Networks Study and some results from simulations of the model

Section 8: Conclusions and Recommendations – Presents conclusions from the Pandemic Influenza Impact on Communications Networks Study and offers recommendations.

Supplemental information is provided in the following appendices:

Appendix A: Acronyms
Appendix B: References
Appendix C: Pandemic Communications and IT Best Practices

2 Stakeholder Involvement

The Pandemic Influenza Impact on Communications Networks Study involves significant industry and government collaboration. Subject matter experts from the fields of communications, cyber security, IT, epidemiology, business continuity planning, financial services, and emergency response have contributed to the study. The study is being coordinated under the DHS Office of Cyber Security & Communications (CS&C) and includes input from the DHS Chief Medical Officer, Federal Communications Commission (FCC), and members of the Financial and Banking Information Infrastructure Committee (FBIIC). On the industry side, representatives from major communications carriers and Internet Service Providers (ISPs) as well as members from the Financial Services Sector Coordinating Council (FSSCC) have been closely involved in the study.

Monthly meetings have been held since October 2006 with industry and government representatives supporting the study. Separate working group style meetings were established with the communications industry representatives and financial services industry representatives. Pandemic plans from several industries have served as context for the overall study.

Communications industry representatives have provided perspective from the network service provider side. In particular, this group has provided valuable insight into the capabilities and engineering tradeoffs present in the design of the commercial communications infrastructure. Financial services representatives have provided perspective from the enterprise and network user side. Subject matter expertise in business continuity planning from the financial service industry has been important in understanding business plans for the pandemic scenario. Industry support helped focus the approach taken in this study. Conclusions and recommendations from the study have been reviewed by the industry and government groups.

The close industry and government partnership in this study follows DHS responsibilities under the President's *National Strategy For The Physical Protection of Critical Infrastructures and Key Assets – February 2003* to "build partnerships with state and local governments and the private sector by designing and implementing its own processes to be open, inclusive, and results-oriented."

3 Methodology

This section provides an overview of the methodology followed by the Pandemic Influenza Impact on Communications Networks Study. The methodology can be broken into three major areas: Potential Congestion Points, Recommended Preparations, and Modeling.

3.1 Potential Congestion Points

In order to evaluate the technical feasibility of widespread telecommuting, the first step was to understand the communications and IT challenges associated with pandemic scenarios. Perhaps the most important feature of a pandemic scenario with regard to the communications infrastructure is the anticipated change in network user behavior. The general trend anticipated is a significant increase in the number of Internet users at home at one time. The potential impact of this trend on the communications infrastructure was examined to identify potential congestion points for telecommuting during a pandemic scenario. Particularly, the feasibility of widespread telecommuting under these assumptions was examined.

3.2 Recommended Preparations

For the potential congestion points identified, industry collaboration helped to identify preparation measures that could better enable the telecommuting strategy to succeed. These preparations were separated into those that could be achieved in the short term and those in the long term. The short term preparations include those that could be taken today, whereas the long term preparations involve leveraging new capabilities anticipated in next generation communications networks.

3.3 Modeling

A model was developed to better understand the relationship between pandemic spread, Internet user behavior, and Internet performance. The model simulated a pandemic spread over a metropolitan area using common epidemiology parameters. The model also examined the potential movement of the Internet user population between home, office, and school locations during a pandemic. A notional metropolitan scale network was federated with network user populations to examine the impact of the change in Internet user behavior on residential Internet access networks. In particular, the ability of telecommuters to perform their functions from residential Internet access networks was examined; specifically the case when increased numbers of Internet users are online during a pandemic. The model was also used to evaluate the potential impact of phased preparations on improving telecommuter performance.

Figure 3.3-1 below illustrates the relationship between the three major activities of the study. Identification of potential congestion points influenced the development of recommended preparations in the short term and long term. Modeling supports both the identification of potential congestion points and recommended preparations by helping to understand the relationship between pandemic spread and Internet use as well as evaluating the potential impact of the recommended preparations on improving telecommuter performance.

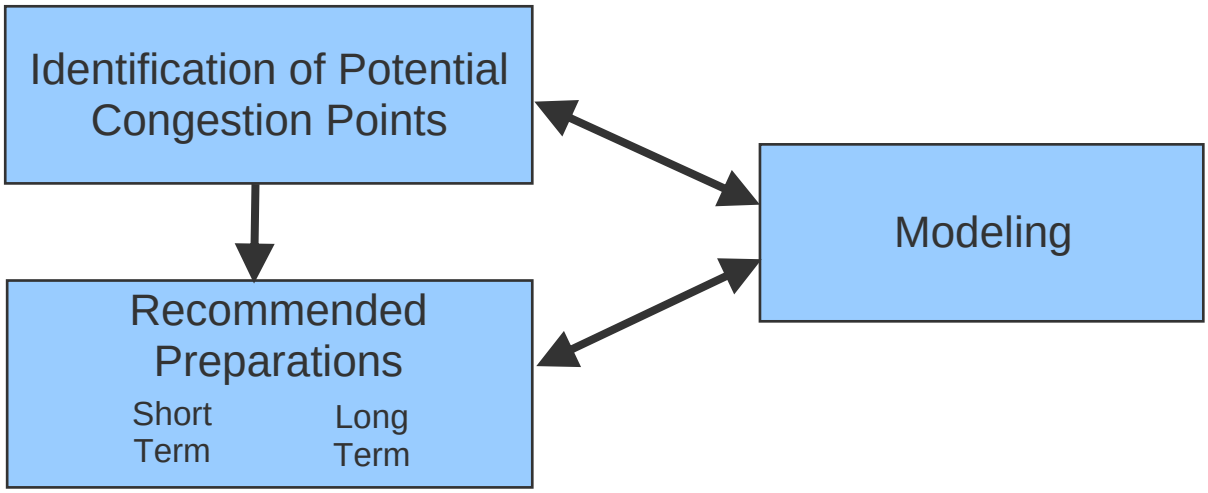


Figure 3.3-1 Study Methodology

4 Potential Congestion Points

In order to examine the potential impact of a pandemic on the communications infrastructure, potential congestion points were identified. Assumptions about the pandemic, communications infrastructure, and the anticipated change in network user behavior are also presented in this section.

4.1 Assumptions

4.1.1 Pandemic Influenza

There are many unknown factors surrounding a pandemic scenario. The unique features of a pandemic outbreak in the U.S. cannot be accurately predicted in advance. However, medical authorities, such as the Department of Health and Human Services, have issued guidelines concerning a potential pandemic scenario for planning purposes. For the purposes of evaluating the potential impact of a pandemic on the communications infrastructure, this study leverages existing assumptions about a potential pandemic and how it might spread through a community.

The first major assumption is that a pandemic may hit the United States with little advance warning and may spread rapidly across the country. This may preclude any large scale shifting of resources or personnel to affected areas. Limited mobility may disrupt domestic and international supply chains. This will hinder significant enhancements to communication and IT capabilities during a pandemic. Multiple waves of a pandemic are likely with each wave lasting 6 to 8 weeks in a community. Illness is anticipated to occur in around 30 percent of the population with rates higher in school-aged children (about 40 percent) and declining with age [7]. These pandemic factors will have a direct impact on the communications infrastructure through the change in network user behavior.

4.1.2 Network User Behavior

During a pandemic, it is assumed that the infection of the disease and need to maintain social distancing will drive changes in network user behavior during a pandemic. HSC advises businesses to plan with the assumption that up to 40 percent of employees may be absent during the 2-week peak of a community outbreak. Public health measures such as quarantines and school closings may increase rates of absenteeism [7].

Individuals who are sick or part of the "worried well" are assumed to spend the majority of their time at home. Many businesses are advising employees to follow telecommuting procedures during a pandemic. This will increase the number of people using the Internet from home, particularly during day time business hours. Most telecommuters are assumed to be connecting to enterprise networks through an encrypted Virtual Private Network (VPN) to perform their work.

School closures will also increase the number of people at home with more children at home and more adults at home supervising children. With limited outdoor entertainment options, children are anticipated to be major contributors to the change in Internet traffic. Video, gaming, and other multimedia application traffic are assumed to increase. Increased demand for health information and emergency services may also increase the overall traffic load during a pandemic.

4.1.3 Communications Infrastructure

In the context of the pandemic scenario with increased network users at home, interviews with communications subject matter experts were used to identify areas of highest risk for telecommuting congestion. ***In particular, consensus was reached that the general areas of highest risk for congestion from the perspective of telecommuting are enterprise networks and residential Internet access networks.*** Communications backbone networks are assumed to be minimally affected in the

pandemic scenario. These backbone networks generally have an ability to support a large surge in traffic load. One backbone provider reported that backbone links are typically maintained at traffic loads not to exceed 45 percent utilization [10]. Additionally, in the network cores, more opportunities exist to balance traffic loads and route around congestion points.

Congestion can occur in many places along a telecommuter's communications path. One cause of congestion can be a mismatch in speed between networks. For example, consider clients on a moderate-speed Ethernet connection (e.g., 10 Mbps) connecting to servers on high-speed networks (e.g., OC-3 155 Mbps). Data flowing from the servers on the high-speed network to the clients on the moderate-speed network may experience congestion at the interface between the networks as illustrated below in Figure 4.1-1. Congestion can also occur in a network node, such as a router or switch, from traffic aggregation in which traffic from multiple input ports is destined for a single output port as illustrated below in Figure 4.1-2. Traffic exceeding the line speed of the output port will be buffered and placed in a queue. Waiting in the queue will add delay to the traffic. Overfilling the queue will lead to packet loss and degraded application performance.

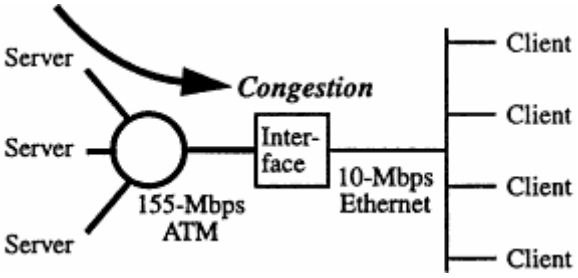


Figure 4.1-1 Congestion Due to Speed Mismatch [11]

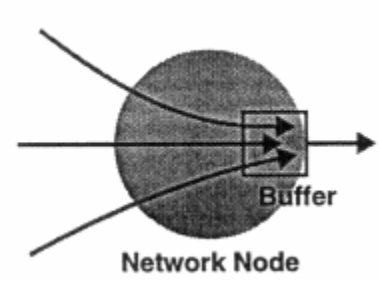


Figure 4.1-2 Traffic Aggregation Congestion in a Network Node [11]

Telecommuters connecting to enterprise networks may be subject to various congestion points in the Internet architecture. Telecommuters have many different access technology options; however, all may be subject to congestion. Figure 4.1-3 indicates some potential congestion points for telecommuters from the two primary sources of congestion, traffic aggregation and speed mismatch. An important take away from the figure is that congestion can occur in many places. The enterprise networks and residential access networks are of highest concern in the pandemic scenario. Still, congestion can occur in other parts of the Internet as well. For example, the Internet is not a single homogeneous domain and the interconnections between ISP domains can be opportunities for congestion to occur.

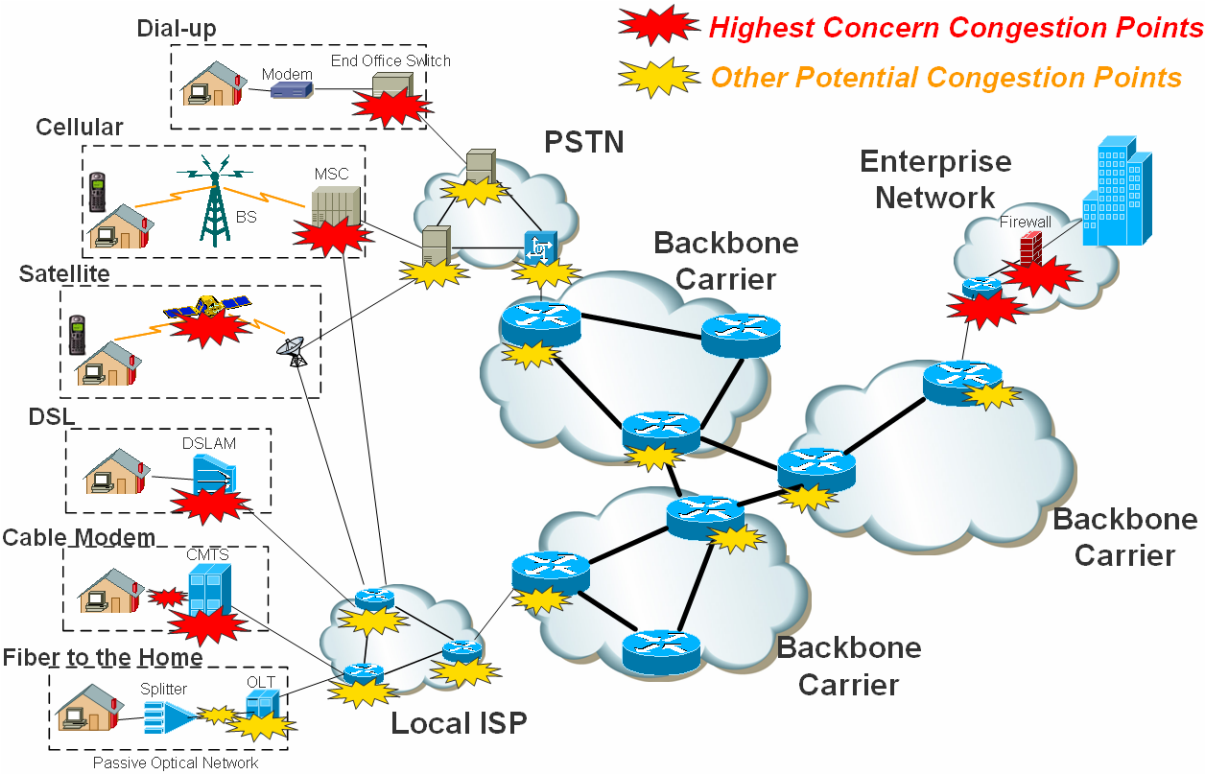


Figure 4.1-3 Potential Telecommuting Congestion Points

4.2 Enterprise Networks

4.2.1 Pandemic Preparedness

Many businesses who have limited reliance on telecommuting today may not be capable of handling the anticipated increase in telecommuting traffic during a pandemic. Enterprise network configurations vary widely across organizations in terms capacity for handling telecommuters. A sampling of a few businesses of various size revealed that gateway connections to enterprise networks were sized to accommodate anywhere from 13 percent to 80 percent of the company's workforce remotely. The HSC *National Strategy for Pandemic Influenza Implementation Plan* May 2006 advises businesses to plan for up to 40 percent absenteeism during the two week peak of a pandemic. Some businesses that currently rely heavily on telecommuting may have robust enterprise networks to accommodate increased telecommuting traffic. Other businesses that utilize minimal telecommuting today may be underprepared to accommodate the increase in telecommuting anticipated during a pandemic.

4.2.2 Potential Congestion Points

There are various congestion points where enterprise networks may not be sized to handle the anticipated surge in telecommuting traffic. Figure 4.2-1 below identifies some potential congestion points for a typical enterprise network configuration.

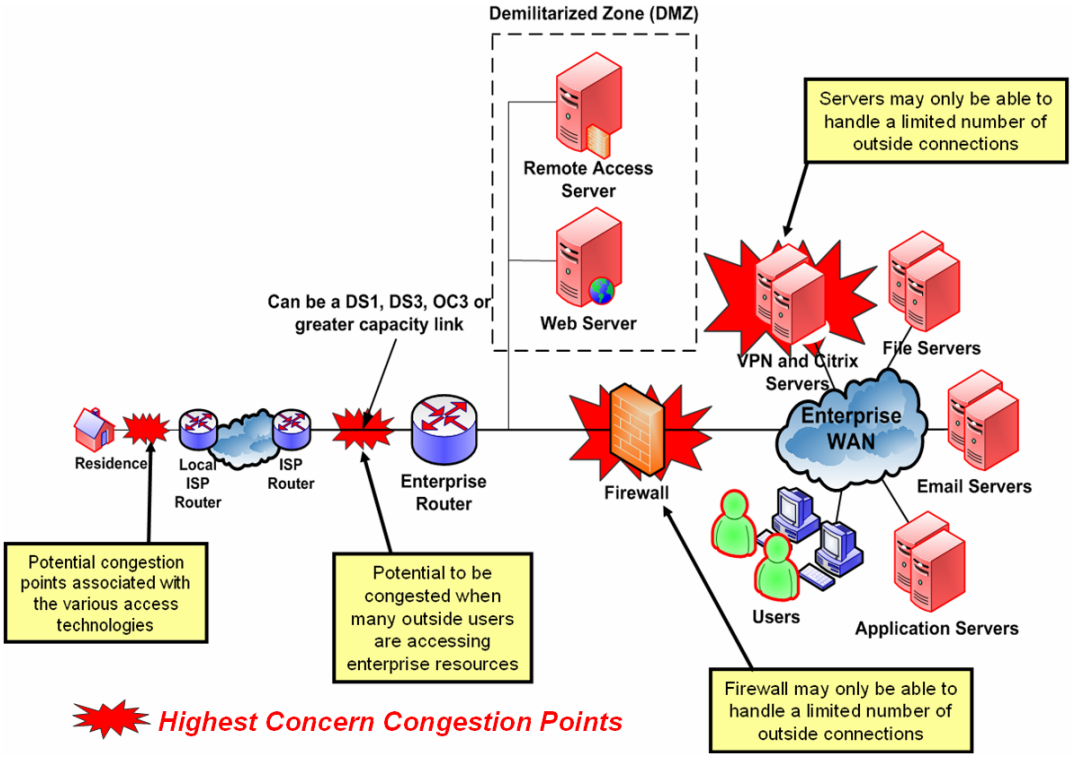


Figure 4.2-1 Potential Enterprise Network Congestion Points [12]

Many telecommuters connect to enterprise networks through VPN software. Once connected, the telecommuter can access corporate resources as if the telecommuter were in the office. The VPN connection process provides authentication and access control to corporate resources. Encryption is often provided by the VPN to provide confidentiality to protect the telecommuter traffic from disclosure.

Increased number of telecommuters during a pandemic may overload certain remote access resources such as firewalls and VPN servers. Limited bandwidth to the Internet from the enterprise network may also constrain the service level provided to telecommuters. Corporate resources that normally serve the office (e.g., file and application servers) should experience a similar traffic load as traffic during a pandemic and are not an area of high concern. However, remote access applications (e.g., webmail) may become overloaded due to an increase in telecommuters using those applications.

4.3 Residential Internet Access Networks

4.3.1 Pandemic Preparedness

During a pandemic scenario, it is anticipated that people getting sick, social distancing measures, and potential mandatory quarantines will dramatically increase the number of people at home for an extended period of time. People at home will include those who are ill at home, caring for a sick family member, watching children, and the worried well. With limited entertainment options and increased interest in health and public safety information concerning the pandemic, communications demand, particularly Internet use, may increase dramatically. Recreational and health information traffic is anticipated to account for the majority of the change in traffic load.

Many telecommuters will be performing their work from residential Internet access networks during a pandemic. Telecommuters have a variety of Internet access options including: dial-up, Digital Subscriber Line (DSL), cable modem, broadband cellular wireless, broadband satellite, and fiber to the home. All of these Internet access technologies are not available in all residential areas; however, many telecommuters have multiple technology options for connecting to the Internet [13]. Broadband penetration in the residential areas is around 50 percent [17] and it is anticipated that the majority of telecommuters will be connecting through broadband access networks.

In these residential areas, telecommuters will be competing with other recreational users for bandwidth. In particular, one of the largest groups of bandwidth consumers is school-aged children. Children also tend to be one of the most infectious groups in terms of disease spread. Communities that decide to close schools during a pandemic will likely see a significant increase in Internet use with children confined to homes likely using the Internet as a mode for entertainment. Statistics from the U.S. Census Bureau estimate that approximately 25 percent of the population in major metropolitan areas is under 18 [18]. Closing schools could thus have a significant impact on the number of Internet users online at once. This surge in Internet traffic from children and other recreational users may affect the ability of workers attempting to telecommute. Congestion on residential Internet access networks may degrade service for telecommuters, particularly those attempting to run applications with real-time requirements.

4.3.2 Potential Congestion Points

Though each basic Internet access technology has different network architectures, all have potential congestion points. Network service providers engineer capacity based on the assumption that only a portion of users will be online at the same time. This allows network service providers to oversubscribe their capacity without any effect on performance during normal operation. Oversubscription ratios have been estimated to range from 10:1 to 100:1 [14, 15, 16]. This means that network service providers may have capacity for approximately one-tenth to one-hundredth of the full capacity offered to their total subscriber population.

During normal operations, this capacity is sufficient to handle peak demand which typically occurs in the early evening when workers and school children return home. During a pandemic scenario, it is anticipated that the number of network users at home will increase and may lead to the peak traffic load being at a different time and significantly above its typical level. If the traffic load increases beyond what the oversubscription ratio allows for, congestion will occur and users will experience degraded service.

Two of the most prevalent broadband Internet access technologies are DSL (~50 percent of broadband population) and cable modem (~41 percent of broadband population) [17]. Figure 4.3-1 below shows some potential congestion points for a typical DSL architecture and Figure 4.3-2 shows some potential congestion points for a typical cable modem architecture. In the DSL architecture, each user has a dedicated connection to the central office. The first potential congestion point is the DSL Access Multiplexer (DSLAM) which multiplexes and switches the many individual DSL connections. In the cable modem architecture, the coaxial local loop is shared among a neighborhood of users and connects to a cable modem termination system (CMTS). The local loop and CMTS are shared resources and are thus potential congestion points. Additionally, both Internet access networks are supported by management and Domain Name System (DNS) servers that can become overloaded.

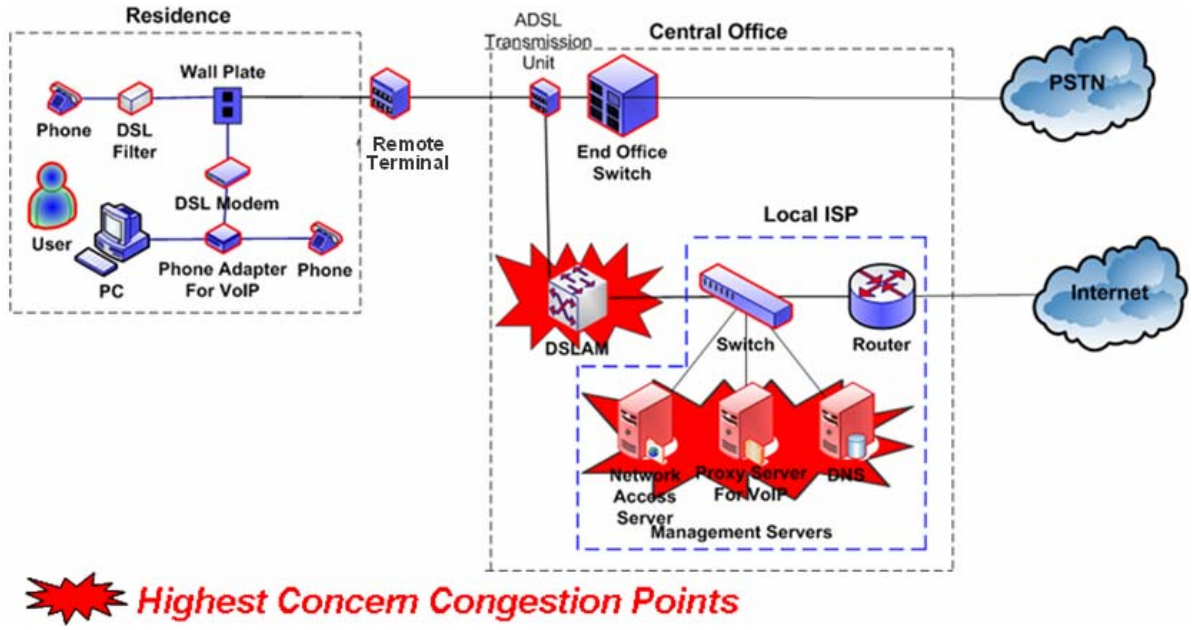


Figure 4.3-1 Potential Congestion Points for Typical DSL Architecture [12]

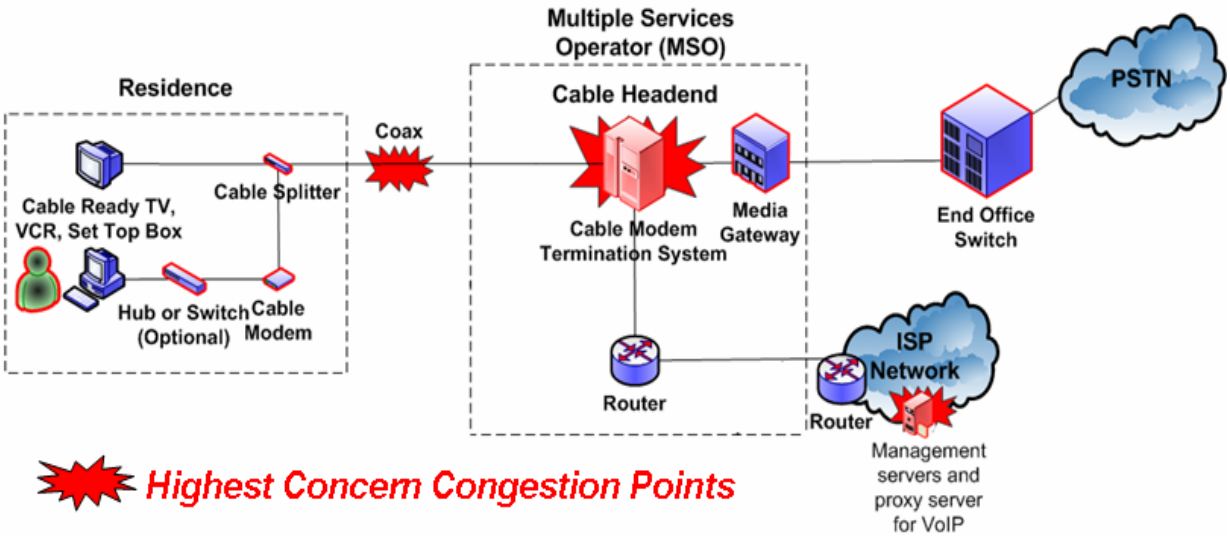


Figure 4.3-2 Potential Congestion Points for Typical Cable Modem Architecture [12]

5 Recommended Preparations

The pandemic scenario poses unique challenges to the nation and to the communications infrastructure. The strategy to mitigate pandemic spread and maintain business continuity through widespread telecommuting may encounter technical issues, as indicated in Section 4 of this report, given the existing communications infrastructure. In particular, existing communications networks may not be sized to meet the unique communications caused by a pandemic scenario. In order to better enable the telecommuting strategy advocated in several national pandemic plans to succeed, a phased approach is proposed.

5.1 Short Term

In the short term, the proposed focus is on providing education and guidance to industry, government at all levels, and the general public on ways to better enable the telecommuting strategy to succeed. This guidance is in the form of communications and IT best practices for planning for a pandemic. The best practices address only communications and IT issues and should be taken in the context of larger pandemic planning efforts. The best practices were developed through industry and government consensus and may need to be tailored to specific local circumstances.

The communications and IT best practices are separated into four categories:

- **Enterprise Network Best Practices** – Guidance for businesses on preparing enterprise IT infrastructure to support an anticipated increase in telecommuting traffic during a pandemic
- **Telecommuter Best Practices** – Guidance for business telecommuters on techniques to maintain business continuity while working from residential access networks
- **General Public Best Practices** – Guidance for the general public on voluntary actions to help reduce potential congestion in residential access networks
- **Network Service Provider Best Practices** – Guidance for network service providers on maintaining operations and existing service levels during a pandemic

Enterprise Network Best Practices

The Enterprise Networks Best Practices are intended to provide guidance to businesses and government on preparing enterprise IT infrastructures to support an anticipated increase in telecommuting traffic during a pandemic. These best practices are focused only on IT issues and should be part of overall pandemic business continuity plans. The full list of Enterprise Network Best Practices is described in detail in Appendix C.

Remote user capabilities are a critical aspect of preparing enterprise networks for a pandemic situation. HSC has advised businesses to plan for up to 40 percent of their employees to be absent during the two week peak of a 6-8 week pandemic wave. ***Businesses should use 40 percent as a guideline, but should assess their particular telecommuting needs during a pandemic situation and size their remote user capabilities appropriately.*** Businesses should also investigate remote management tools to ensure that network managers who may be absent during a pandemic can continue to manage the organization's enterprise networks.

Another important area of the Enterprise Network Best Practices is cyber security. Businesses will increase their reliance on communications and IT services to maintain business continuity during a pandemic. This increased reliance on communications and IT services may increase an enterprise's cyber risk. With reduced support staff due to the pandemic, businesses may also have decreased capabilities to respond to cyber incidents. Additionally, cyber threats may increase during a pandemic as attackers may view the situation as an opportune time to increase attacks. Businesses

should work to improve their cyber security posture for a pandemic scenario. Some example cyber security best practices are listed in Appendix C.

Telecommuter Best Practices

The Telecommuter Best Practices are intended to provide guidance to business telecommuters on techniques to maintain critical business functions while working from residential Internet access networks. The full list of Telecommuter Best Practices is described in detail in Appendix C.

Residential Internet access networks are designed to provide moderate bandwidth, best effort service. No guarantees are provided for the availability and performance of these networks. These networks were designed primarily for recreational use, not for high bandwidth, business critical applications. ***Employees who plan to telecommute during a pandemic and are truly critical to business operations should not rely on best effort, residential Internet access.*** These critical users should consider obtaining a premium or dedicated service that offers some level of availability and performance guarantees. Critical users should also consider obtaining multiple connectivity options (e.g., DSL, cable modem, wireless broadband) for redundancy in case of network congestion. Any such services should be installed prior to the outbreak of a pandemic as new service installations may be limited during a pandemic.

Despite the lack of guaranteed service from residential access networks, the need for widespread telecommuting during a pandemic will force some users to use this best effort service for business purposes. Residential access networks will be relied upon to support important business applications. Facing the constraints of residential access networks, telecommuters can employ several methods to work more efficiently during a pandemic.

Bandwidth saving practices employed by telecommuters may enable them to perform functions more efficiently and also contribute less to network congestion. Examples of bandwidth saving practices include performing large data transfers at night, logging off corporate VPN connections when not in use, and using Instant Messaging applications instead of voice communications.

Increased numbers of employees working from home instead of the office during a pandemic also has cyber security implications. Employees normally protected by corporate security mechanisms must now rely on the security of their home networks. Telecommuters should follow cyber security procedures for their home networks including: installing a firewall, using anti-virus programs, and keeping system and applications software patched.

General Public Best Practices

The General Public Best Practices are intended to advise the general public on voluntary actions to help reduce traffic load, particularly on residential Internet access networks. The full list of Enterprise Network Best Practices is described in detail in Appendix C.

During a pandemic, changes in general public behavior will likely account for the vast majority of change in traffic on communications networks. Social distancing measures, imposed quarantines, and school closures may all result in a large percentage of the general public at home in a given area for an extended period of time. With fewer entertainment options and increased demand for information concerning the pandemic, communications traffic in residential areas is anticipated to significantly increase. This increase in communications traffic may impact telecommuters who are competing for bandwidth on residential access networks. For example, telecommuters may experience increased delay in downloading files or may be unable to use certain real-time

applications due to large numbers of other residential users watching online videos or children playing online games.

Limiting non-critical recreational traffic, particularly during day time work hours, will be key to enabling the pandemic telecommuting strategy to succeed. In particular, the general public may be asked to voluntarily limit streaming media, gaming, peer-to-peer (P2P), and other bandwidth intensive applications during day time work hours. The general public will also be encouraged to follow bandwidth saving practices such as using broadcast news sources (e.g., TV, radio) in place of online news and configuring web browsers to block multimedia content.

Voluntary actions taken by the general public have significant potential to reduce surge traffic load that may be seen during a pandemic. The primary challenge with achieving the effect of these voluntary actions is compliance by the general public. Parents or heads-of-household could be asked to enforce restrictions on online usage, particularly use by children. Businesses' pandemic plans should consider including guidance to telecommuters on enforcing restrictions for online use in their households.

Network Service Provider Best Practices

The Network Service Provider Best Practices are intended to advise network service providers on maintaining operations and existing service levels during a pandemic. Most network service providers have well established plans for maintaining and repairing service during emergency situations, ranging from individual fiber cuts to widespread damage of physical infrastructure by a natural disaster or terrorism. The best practices listed in Appendix C are intended to illustrate some of the unique characteristics for network service providers of a pandemic situation in contrast to other emergencies. Many network service providers have developed pandemic plans and may already be taking many of these actions.

Unlike many emergency and contingency plans by network service providers, a pandemic situation does not involve any physical damage to the network. Emergency plans focusing on restoration and temporary provisioning do not apply as well to a pandemic. Instead, the major impact on network service providers will likely be an extended surge in traffic and degraded workforce. The surge in traffic will come primarily from increased telecommuters and the general public on residential access networks. ***Network service providers will also be affected by the spread of a pandemic and will be operating with a reduced workforce. This will likely limit the ability of network service providers to respond to any surge in traffic and provision new capacity.***

With a reduced workforce, some network service providers have indicated they will focus on maintaining existing services as opposed to provisioning new services during a pandemic. Remote network management tools may be important for network service providers to continue to operate with a reduced workforce. Network service providers should also be aware of supply chain disruptions, particularly regarding high-tech equipment from overseas, which could affect their business operations. Network service providers may consider examining whether their inventories will sustain a potential 6-8 week supply chain disruption.

5.2 Long Term

In the long term, critical telecommuters in a pandemic scenario may be able to take advantage of priority services in next generation networks. Capabilities are being developed by the DHS National Communications System (NCS) in coordination with the communications industry to provide priority services for national security and emergency preparedness (NS/EP) personnel in next generation networks.

NCS is directed to coordinate "the planning for and provision of national security and emergency preparedness communications…under all circumstances, including crisis or emergency" [19]. NCS currently offers a range of NS/EP communications services including Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP). GETS provides emergency access and priority processing in the public switched telephone network. WPS provides priority cellular network access. TSP provides priority restoration and provisioning of telecommunications circuits for critical users. These services are available to organizations that perform NS/EP functions including those in the private sector critical to "maintaining public welfare and national economic posture."

One major shortcoming of GETS and WPS for the pandemic scenario is that these services provide priority treatment only for voice and low-speed (e.g., dial-up) data. No comparable service currently exists for broadband applications. The Internet was originally designed to provide best effort, non-differentiated service. While this model still largely governs the operation of the Internet, there is increasing interest and activity by network service providers in incorporating quality of service (QoS) and service differentiation into next generation networks. Many network service providers today offer business class services, such as MPLS VPNs and leased lines, which can provide QoS as well as logical and physical traffic separation from other best effort traffic on the provider's network. However, these mechanisms do not apply to Internet traffic which may traverse several different networks on the Internet.

NCS is working to expand the capabilities of GETS and WPS into next generation networks. The objective is to make priority NS/EP communications possible not only for voice telephony, but also for other services such as video teleconferencing, email, and Internet access. These capabilities could potentially be leveraged to support business continuity during a pandemic by providing priority to critical telecommuter groups if the required features are designed into the commercial communications infrastructure. Private industry members are currently eligible under NS/EP criteria for priority services when sponsored by a government organization. The widespread eligibility for critical telecommuters in a pandemic scenario may need to be examined. The current NS/EP user base is relatively small at around 161,000 GETS users and 46,000 WPS users. The potential NS/EP user base for next generation networks has been estimated to be on the order of several million.

The greater than order of magnitude increase in NS/EP user support suggests the priority mechanisms may be scalable to accommodate a potential additional increase in users for the pandemic scenario. The pandemic scenario is unique as an emergency situation in its widespread impact and extended time frame. Telecommuters critical to maintaining business continuity in critical infrastructures may be a large user group in a nation-wide pandemic scenario. These telecommuters may be running bandwidth intensive applications at least 8 hours a day over a 6-8 week pandemic. The service requirements to support critical telecommuters during a pandemic may place an additional burden on priority services in next generation networks. Priority services in next generation networks may need to be examined for their ability to meet the unique challenges of a pandemic scenario.

The details of the enhanced NS/EP broadband priority services are currently in development. Timelines from the program estimate that these services are still at least several years away with initial capabilities anticipated around 2011-2012.

6 Outstanding Issues

6.1 Worst Case

Both the short term and long term preparations proposed above have potential challenges in addressing the communications and IT issues associated with the pandemic threat. The short term preparations of best practices are founded on the assumption of voluntary compliance by industry and the general public. A major uncertainty is the level of voluntary compliance. It is particularly important for the general public to follow the best practices related to limiting non-critical recreational traffic during day time working hours. Changes in general public behavior during a pandemic is expected to be the primary cause of changes to the traffic load observed on residential Internet access networks. If compliance with the best practices is not high enough, telecommuters may face widespread congestion and business continuity may be impacted.

The long term preparations include leveraging priority services in next generation networks. The primary issue with this proposal is that the details of these services are still in development and will not be available for several years. Eligibility and scalability of priority services for critical telecommuters in a pandemic scenario may also need to be examined.

Modeling results described below suggest that potential pandemic scenarios exist in which the severity of pandemic and/or low level of compliance with communications and IT best practices may still lead to network congestion. The best practices are primarily aimed at reducing the background traffic levels on residential Internet access networks. ***The Federal government should continue to work with industry to investigate mechanisms that could be implemented when voluntary compliance with best practices is not enough to enable to the telecommuting strategy to succeed.***

A key component of investigating worst case mechanisms is understanding when these mechanisms should be employed. The purpose of the mechanisms is to reduce congestion so that critical telecommuters can achieve sufficient service in order to limit the impact to business continuity. ***Since congestion is anticipated to occur locally and at different times in different locations, a method of monitoring and reporting of telecommuting performance of critical infrastructures may be necessary.*** If specific actions are to be taken in response to particular congestion conditions, a method of identifying when those conditions occur will be needed. Monitoring and reporting systems similar to those established for Y2K could be investigated for the pandemic scenario.

6.2 Cyber Security

In the communications industry, cyber security is an area of considerable attention today. The communications industry has spent considerable resources in recent years to improve cyber security posture. The pandemic scenario involves a significant shift in the locations of the network user population. Anticipated changes in network user behavior during a pandemic may lead to a different cyber security environment and increased risk to telecommuters and network service providers.

Workplace absenteeism and the need to maintain social distancing will likely increase the reliance of businesses on communications and IT services in a pandemic scenario. This increased reliance may heighten cyber risk for businesses, telecommuters, and general public Internet users. With reduced support staff due to the pandemic, businesses may also encounter decreased capabilities to respond to cyber incidents. Attackers may also view the U.S. as vulnerable and may increase attacks during a pandemic. Employees normally protected by corporate firewalls must now rely on the security of their home networks.

An in-depth analysis of pandemic related cyber security issues is outside the scope of this study. As a partial assessment, traditional cyber security best practices were collected for telecommuters and enterprise networks. ***A more detailed assessment may be required to identify any unique characteristics of the cyber security environment for a pandemic scenario.***

7 Modeling

7.1 Purpose

As part of the study, a model was developed to better understand the relationships between pandemic spread, Internet user behavior, and Internet performance. The purpose of studying these relationships was to better understand the magnitude and dynamics of the change in Internet traffic that may be observed during a pandemic as well as analyze the effect of communications and IT best practices on reducing congestion.

7.2 Scope

The dynamics between pandemic spread and Internet user behavior are assumed to occur primarily at a metropolitan level. The pandemic is anticipated to spread across the country due to people traveling between major cities. Within metropolitan areas, population densities and mixing between populations are anticipated to largely drive the pandemic spread. From the perspective of telecommuters, the majority of communications traffic is anticipated to be between the telecommuter and the enterprise network and therefore mostly confined within the metropolitan area. Thus, the intrinsic scale of understanding the relationships between pandemic spread, Internet user behavior, and Internet performance is assumed to be at a metropolitan level.

Defining the scope of the model is important for interpreting the results of the model. The model is intended to be at the scale of a major metropolitan area in terms of people and network traffic sources. The model can fully represent the population in terms of disease spread and is within an order of magnitude for network traffic sources (limited by hardware memory). The model uses census and Department of Transportation data from the Chicago metropolitan area [22]. However, results from the model are expected to be extensible to other metropolitan areas of comparable size. Since detailed network architectures from the network service providers are tightly held, open source information and engineering best practices were used to construct a typical network architecture model. The network architecture model focuses on representative residential Internet access networks. Internet backbones and enterprise network are assumed to perform at a given level. Figure 7.2-1 describes the scope of the constructed model.

What the Model IS	What the Model IS NOT	Consequence
▪ Metropolitan scale model ▪ Uses some data and assumptions about Chicago to construct a representative metropolitan area model	▪ National scale model ▪ Detailed model of the specifics of Chicago	▪ Pandemic spread and network use dynamics mostly at metro level ▪ Results not specific to any geographic area, extensible to metro areas of comparable size
▪ Model of residential Internet access networks (initial phase – DSL)	▪ Model of communications backbones or enterprise networks	▪ Areas of greatest concern are access and enterprise networks in metro area ▪ Enterprise networks vary widely so unable to model
▪ Discrete event simulation of subset of network user population ▪ Large scale network modeling which abstracts some network details ▪ Network model details based on open source information and engineering best practices	▪ High fidelity model of every network device and every network user ▪ Actual carrier architecture	▪ Notional network architecture so not necessarily representative of any carrier's architecture ▪ Some network protocol behaviors may be abstracted and perform slightly differently
▪ Capability to evaluate the potential impacts of implementing preparation measures on relieving network congestion	▪ Capability to analyze the technical, business, or legal issues associated with implementing preparation measures	▪ No assessment of mechanisms to implement best practices or other preparation measures

Figure 7.2-1 Model Scope

7.3 Overall Architecture and Design

This section provides an overview of the modeling architecture constructed. The overall model is an agent-based model and performs discrete event simulation. The modeling architecture can be logically separated into three components: Pandemic Spread, Network Users, and Network. The basic premise behind the model is that the Pandemic Spread component simulates the disease spreading through a metropolitan area. Based upon getting sick and other factors, the Network Users component has agents decide whether to remain at work/school or to go home. The Network Users component also assigns a traffic profile to each type of agent. When these agents are at home they put their traffic profile onto the network. The Network component then simulates the conditions of a typical access network in response to the offered traffic load.

7.3.1 Pandemic Spread

The Pandemic Spread component is intended to simulate the spread of a pandemic across a metropolitan area. The purpose of the Pandemic Spread component in the overall modeling architecture is to move individuals through the different stages of the disease in order to cause individuals to change location. Since the model is ultimately examining the impact on the communications network, the utility of the Pandemic Spread component is essentially just to move potential network users from work and school locations onto residential access networks.

Several infectious disease models have been developed and there is ongoing debate on the representation of certain epidemiology parameters. For the purposes of this study, many of these details are considered irrelevant as they will not largely affect the gross number of people infected in a given area. The Pandemic Spread component used was based largely on seminal epidemiology research [21]. Spread of the disease follows the general Susceptible-Exposed-Infected-Recovered (SEIR) algorithm. In the SEIR algorithm, an individual contracts the disease through its interaction with other agents and passes through the four stages of the disease based on a variety of disease parameters such as time of incubation, time of contagion, time of recovery, mortality rate, etc.

The SEIR algorithm was implemented through mixing in home, office, and school locations in the metropolitan area. The home locations were derived from data on census tract populations from the Year 2000 census. Office and school locations were derived from data from the Department of Transportation that showed morning commuting patterns between census tracts [22]. The Pandemic Spread component was calibrated to the homogeneous case to ensure proper implementation of the SEIR algorithm.

7.3.2 Network Users

The Network Users component was responsible for two major aspects of the model: agents deciding whether or not to go home and the users' network traffic profiles. Agents may decide to go home based on a number of factors. The primary driver is the infection of the disease. Agents who begin feeling sick may be assumed to go home. Agents may also decide to go home based on having to take care of a sick family member or being part of the worried well and attempting to avoid contracting the disease.

Each type of agent was assigned a user traffic profile. Initially, four categories of users were created: At Home User, Telecommuter, Financial Telecommuter, and Child User. Public source information on typical network traffic was used to construct a traffic profile for each category. The traffic profiles make assumptions about the type of applications run and how long to run each application. These assumptions were aggregated into an average desired throughput rate for each user category. Real world data from a recent Federal Reserve Board telecommuting exercise was used to verify assumptions about telecommuter traffic profiles. All of this information was used to create the traffic load for the Network component.

7.3.3 Network

The Network component was intended to represent typical access networks in a metropolitan area. The Network component leveraged several open source datasets to create the representative network. The University of Washington 'Rocketfuel' dataset contains real-world ISP topologies collected from traceroutes. This data was used to create the topology of 10 ISPs with 3000 routers spanning a metropolitan area [23]. The last mile access portion of the network was constructed based on market research of typical equipment and configurations deployed. For example, for the DSL last mile architecture, market research on the DSLAM vendor market and their typical configurations was used. Link capacities in the last mile were selected using oversubscription estimates from industry analysis. These oversubscriptions have been estimated to range anywhere from 10:1 to 100:1 [14, 15, 16].

In order to construct a metropolitan scale network model, the Network component was constructed on the Rensselaer Optimistic Simulation System (ROSS) platform. This platform abstracts some communications protocol details but preserves their basic functions. The Network Model was scaled to accommodate more than 200,000 discrete event traffic sources. The limitation on the number of traffic sources was imposed by the hardware memory available and is not a function of the model architecture. The use of 200,000 discrete event traffic sources is within an order of magnitude of the approximately 2 million people in the Chicago area with Internet access.

The Network component took the agent locations and corresponding traffic profiles as input to generate the traffic load for the network. The discrete event simulation mapped a separate traffic flow to every network user. The status of the network can be measured at various points in the Network Model. For example, each router can report queuing delays at any port. Network user performance in terms of throughput can be measured for every user.

7.4 Initial Results

7.4.1 Pandemic Parameters

The first major question addressed with the model was: How do pandemic conditions affect Internet traffic? An analysis of variance was performed to identify whether the pandemic parameters of Initial Percent Sick, Incubation Duration, Degree of Contagion, Symptomatic Duration, and Mortality Rate would increase, decrease, or have no effect on the network traffic load. The relative impact on the network traffic load was analyzed by measuring the peak home network user population under the different pandemic cases. The graphs in Figure 7.4-1 show the effect of the pandemic parameters on the peak home network user population. Note the base case of *no pandemic* consists of 38 percent of the population as home network users. These base case users, derived from census data, are those who do not normally commute to work or school during the day.

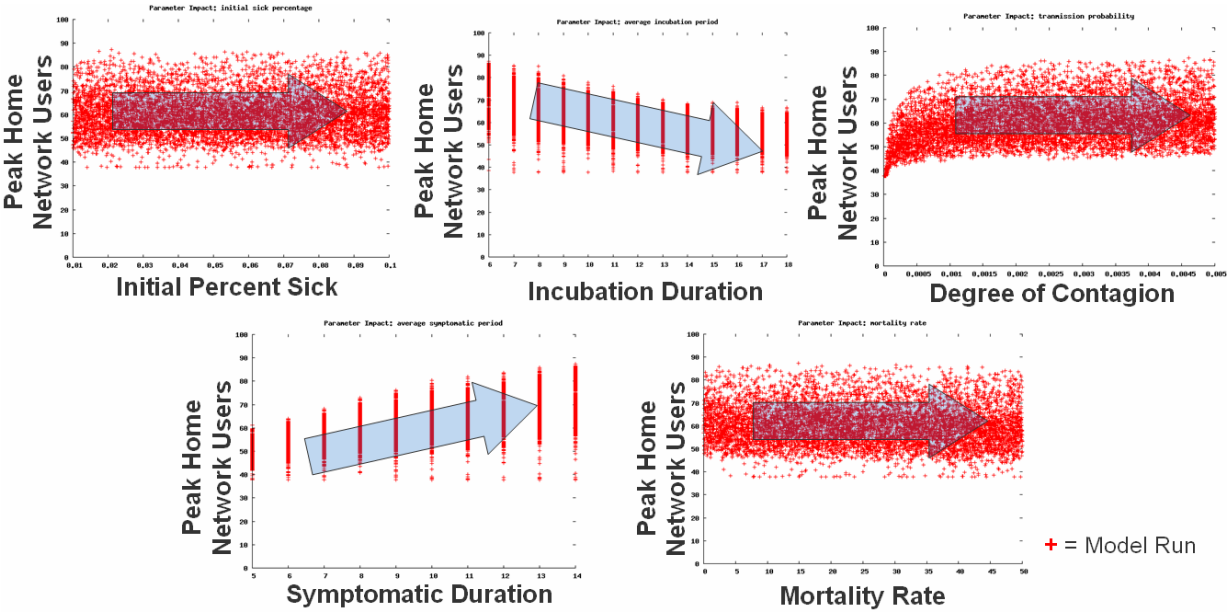


Figure 7.4-1 Pandemic Parameters

Examination of Figure 7.4-1 reveals that the pandemic parameters have different effects on the peak home network user population in the model. The effects can be summarized as:

Increased Network Users: Symptomatic Duration

Decreased Network Users: Incubation Duration

No Effect: Initial Percent Sick, Degree of Contagion, Mortality Rate

The effects of the parameters must be interpreted in the context of the model formulation. Symptomatic duration is expected to increase the peak home network population as the population will be sick for a longer time and thus home for a longer time. Incubation duration is expected to decrease the peak home network as the population will tend to get sick at different times and thus be at home at different times. Within a reasonable range, initial percent sick and degree of contagion on average appear to have no effect on the peak home network user population. Mortality rate also has no effect on the peak home network user population. In the model formulation, network users who become sick and go home must follow one of two paths: recover and go back to work, or become

deceased. In either case, the network user is no longer on the home network. Thus, mortality rate has no effect on the peak home network user population. The severe Spanish pandemic of 1918 had a mortality rate of approximately 2.5%.

Taken together, these results point to the fact that there is a significant degree of uncertainty regarding how the pandemic will affect the home network user population. The uncertainty of the specific disease parameters that will accompany an actual pandemic affects the uncertainty of the home network user population that will be observed. As more epidemiology information is learned about a potential pandemic, a better prediction of the home network user population and subsequent traffic load on the network may be made.

7.4.2 Pandemic Scenarios

In order to further quantify the potential impact of a pandemic on the communications infrastructure, several pandemic scenarios were selected to analyze network performance. From the perspective of impact to the communications infrastructure, the home network user population during the pandemic is the most important factor. In this study, the pandemic scenarios are characterized based on their effect on the home network user population.

Three pandemic scenarios of particular interest include a low absenteeism pandemic, 40 percent absenteeism pandemic, and a high absenteeism pandemic. The low and high absenteeism cases correspond to 20 percent and 90 percent absenteeism of the working population respectively. The low and high absenteeism cases are intended to give a lower and upper bound for reasonable pandemic, worried well, and quarantine parameters.

40 percent absenteeism corresponds to the HSC guideline that businesses should plan for 40 percent absenteeism. 90 percent absenteeism is an extreme case intended to examine the limit of impacts to the network infrastructure from increased traffic load. While 90 percent absenteeism may be unlikely, the results from this case may approximate conditions during localized quarantine conditions. Figure 7.4-2 below shows results for the low absenteeism case, Figure 7.4-3 shows results for the 40 percent absenteeism case, and Figure 7.4-4 shows results for the high absenteeism case.

For each pandemic scenario, three graphs are displayed: Pandemic Spread, Network Users, and Network Performance. The Pandemic Spread graph shows the percentage of the population that contracts the disease as they progress from Susceptible to Exposed to Infected to Recovered/Deceased. The Network Users graph shows how the home network user populations change as the disease spreads across the metropolitan area. Home network users are categorized into four groups with different traffic profiles:

- Type 0 At Home – Network users who are normally at home
- Type 1 Workers – Telecommuters working from home locations
- Type 2 Finance – Financial industry telecommuters working from home locations
- Type 3 Children – School-aged children home from school

The Network Performance graph shows end user network performance during the pandemic for each home network user category. For analysis purposes, network user performance is categorized into Levels based on the ability of users to achieve their average desired bit rate.

- Level 0 – Network users are able to achieve desired bit rate
- Level 1 – Network users achieve less than desired bit rate but at least 1/2 desired bit rate
- Level 2 – Network users achieve less than 1/2 but greater than 1/10 desired bit rate
- Level 3 – Network users unable to communicate due to TCP maximum backoff time

7.4.2.1 Low Absenteeism Scenario

In the low absenteeism pandemic scenario, 20 percent of the working population is absent during the peak of the pandemic which causes the home network user population to increase slightly. This results in a small percentage of the population experiencing congestion during the peak of the pandemic. For the telecommuter populations (Type 1 and Type 2), over 80 percent do not experience any degradation in network throughput even during the peak of the pandemic wave. Of the telecommuters that do experience congestion, those with lower bandwidth requirements (Type 1) are generally able to achieve at least 1/2 their desired throughput. Telecommuters with higher bandwidth requirements (Type 2) experience slightly more congestion during the two week peak of the pandemic. ***In the low absenteeism pandemic scenario, the telecommuting strategy is anticipated to be successful for the majority of telecommuters.***

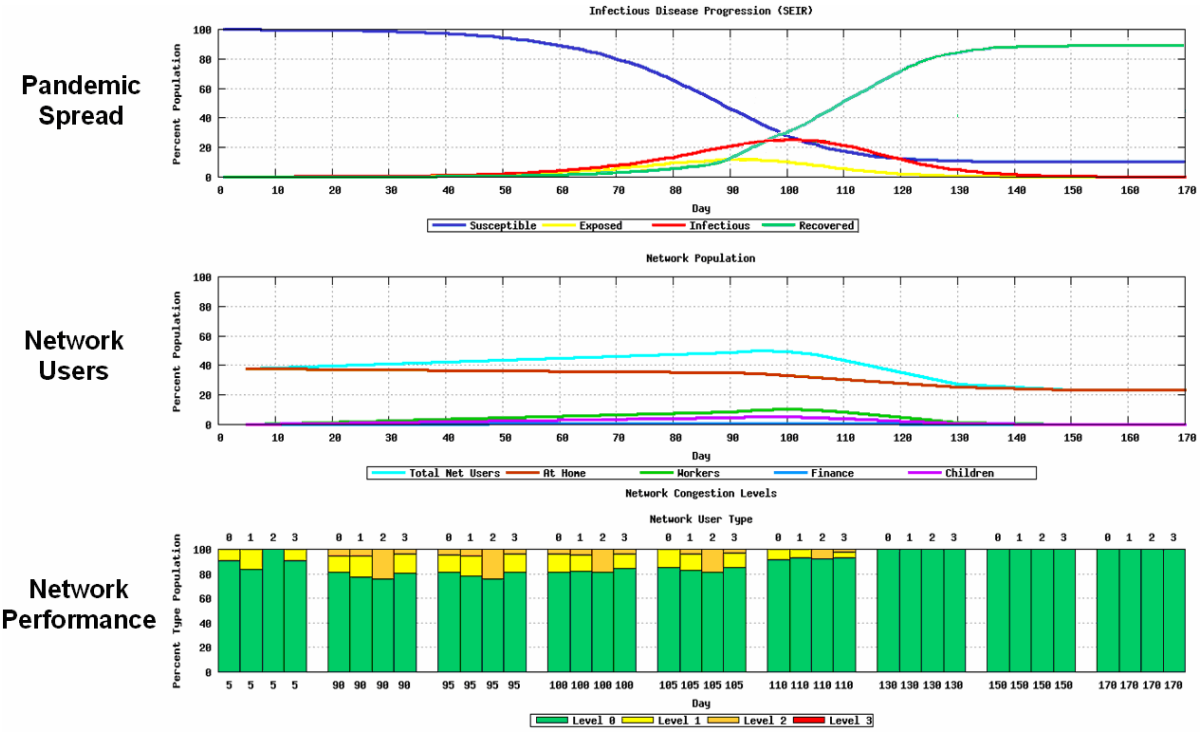


Figure 7.4-2 Low Absenteeism Pandemic Scenario

7.4.2.2 40 Percent Absenteeism Scenario

In the 40 percent absenteeism pandemic scenario, network user congestion is observed to be much greater and more widespread. During the two week peak of the pandemic, over 90 percent of network users in each user category experience degraded throughput and are in at least Level 1 congestion. Over 50 percent of telecommuters (Type 1 and Type 2) achieve less than 1/2 their desired throughput and are in Level 2 congestion during the peak. In Level 2 congestion, nearly all real time applications may be unusable and most non-real time applications will be severely impacted. During this time, businesses may face a significant impact to maintaining business operations remotely. ***In the 40 percent absenteeism pandemic scenario, the telecommuting strategy is expected to be significantly impacted for most telecommuters during the peak of the pandemic.***

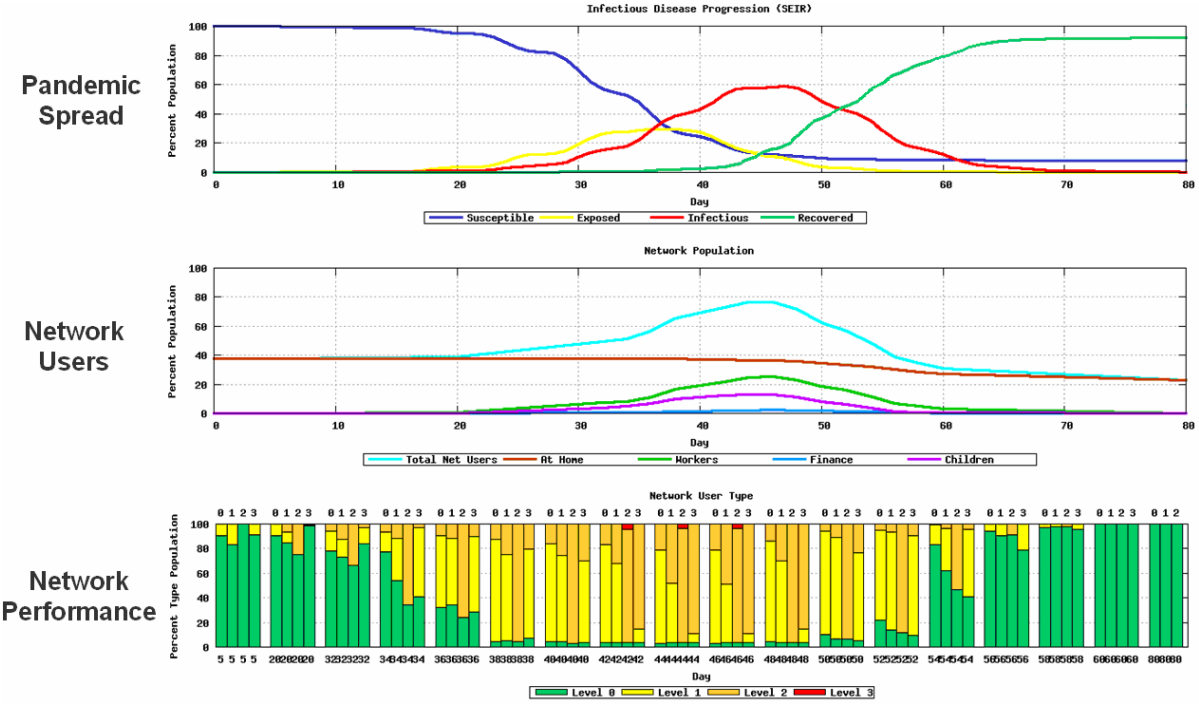


Figure 7.4-3 40 Percent Absenteeism Pandemic Scenario

7.4.2.3 High Absenteeism Scenario

In the high absenteeism pandemic scenario, 90 percent of the working population is absent during the peak of the pandemic. While 90 percent absenteeism may be unlikely, the results from this case may approximate conditions during localized quarantine conditions. With significantly more people on residential networks, home network users experience even higher levels of congestion. During the peak of the pandemic, nearly all Type 0, 1, 2, 3 users experience at least some level of congestion. Nearly 90 percent of the telecommuter populations (Type 1 and Type 2) experience Level 2 congestion at some point. This may significantly impact real time applications for telecommuters. Some high bandwidth telecommuters enter Level 3 congestion in which even non-real time applications may face significant performance issues. ***In the high absenteeism scenario, the telecommuting strategy is expected to be unusable for the majority of telecommuters during the peak of the pandemic.***

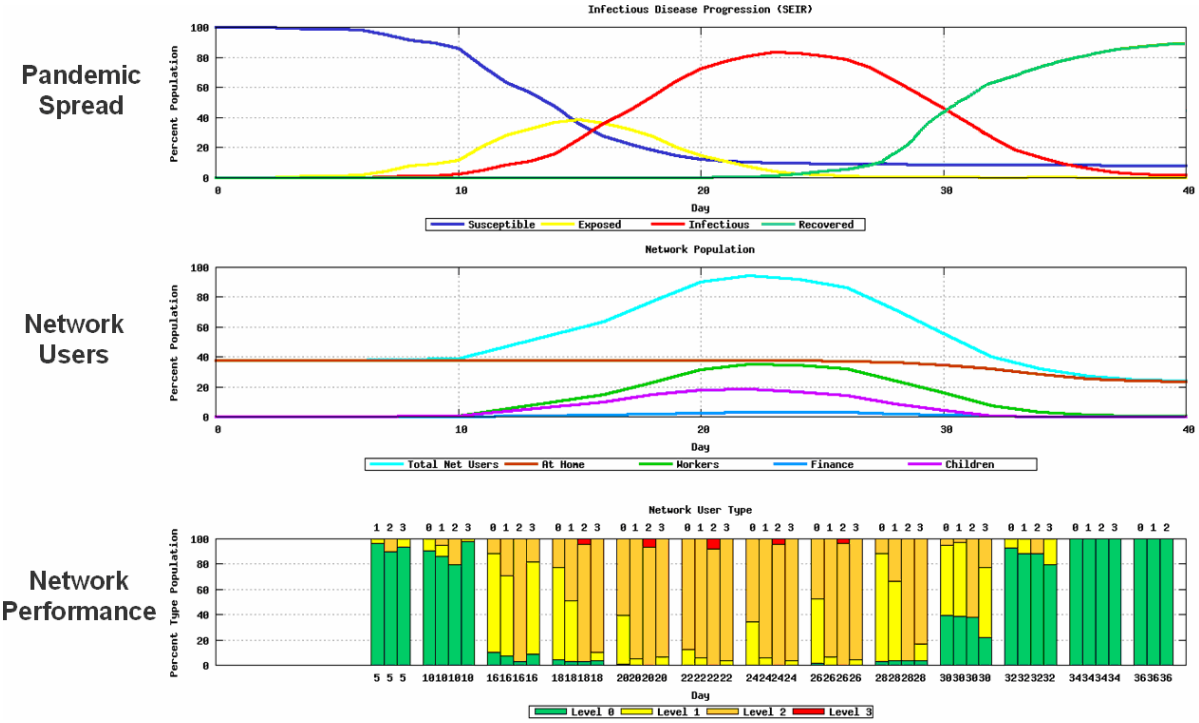


Figure 7.4-4 High Absenteeism Pandemic Scenario

7.4.3 Best Practices

The effect of implementing Communications and IT Best Practices on the network traffic load during a pandemic was also investigated. These were mostly focused on reducing the background traffic load by asking the general public to voluntarily limit non-critical recreational traffic particularly during day-time working hours. The best practices were simulated in the model by changing network user traffic profiles.

Two pandemic scenarios of particular interest were examined, 40 percent absenteeism and a high absenteeism case. The best practices that appeared to have the greatest impact on reducing the background traffic load were limiting video traffic and limiting gaming traffic. These individual best

practices as well as the sum of all best practices are plotted in Figure 7.4-5 for the 40 percent absenteeism scenario and Figure 7.4-6 for the high absenteeism scenario.

One interesting result for the 40 percent absenteeism case is that full compliance with all the best practices is enough to bring nearly all types of home network users back to Level 0. These best practices mostly focus on reducing the background traffic load from the general public. In other words, if the general public can be convinced to reduce time online and limit bandwidth intensive applications, then telecommuters may be able to obtain their desired performance.

However, there are still scenarios in which the best practices may not be enough and widespread congestion can still occur. As seen in Figure 7.4-6, telecommuters in the high absenteeism case may still experience congestion during the peak of the pandemic even with high compliance with the best practices. Nearly half of high bandwidth telecommuters (Type 2) experience Level 2 congestion during the peak of the high absenteeism pandemic. Low compliance with the best practices may also result in many telecommuters experiencing congestion. Figure 7.4-7 shows the effect of varied compliance with all the best practices in the 40 percent absenteeism scenario. At low levels of compliance, congestion experienced by telecommuters is not dramatically different than in the *no best practices* base case. At relatively high levels of compliance, the duration of the congestion conditions begins to shrink. Though at even 75 percent compliance, over half of all telecommuters (Type 1 and Type 2) have some throughput degradation and experience at least Level 1 congestion during the peak of the pandemic. ***Thus, a high rate of compliance with the best practices may be necessary to enable the telecommuting policy to succeed if no other actions are taken.***

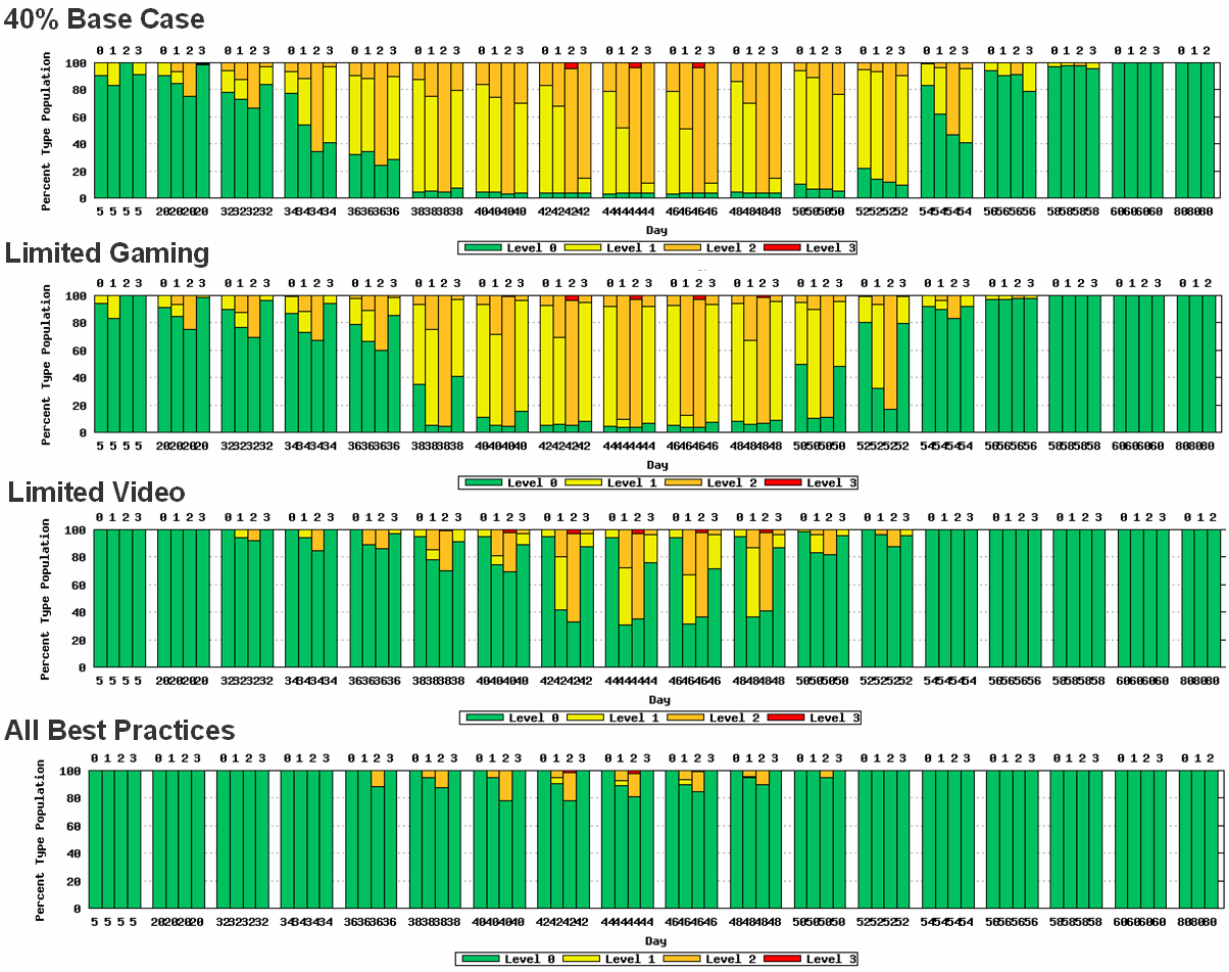


Figure 7.4-5 Best Practices in 40 Percent Absenteeism Scenario

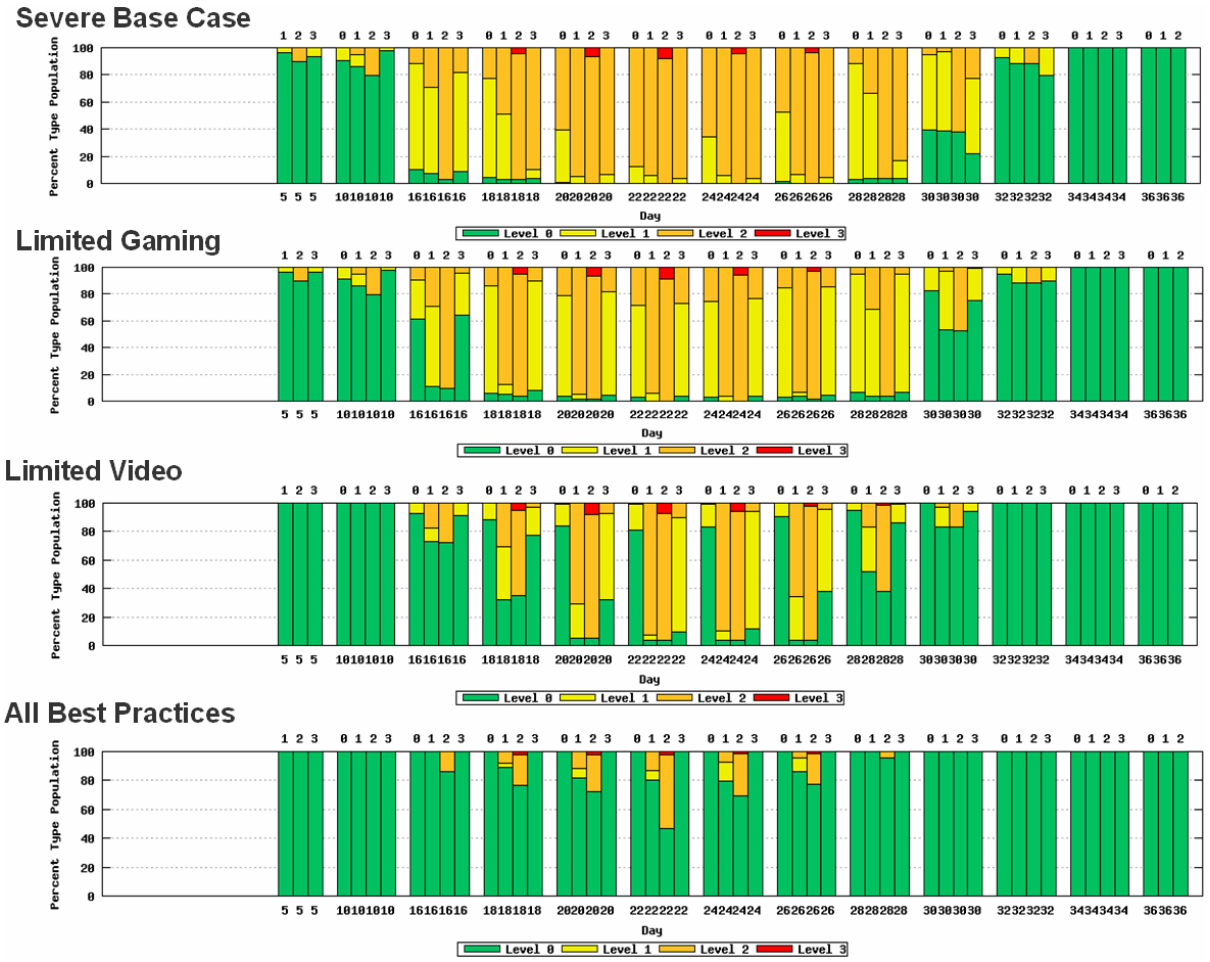


Figure 7.4-6 Best Practices in High Absenteeism Pandemic Scenario

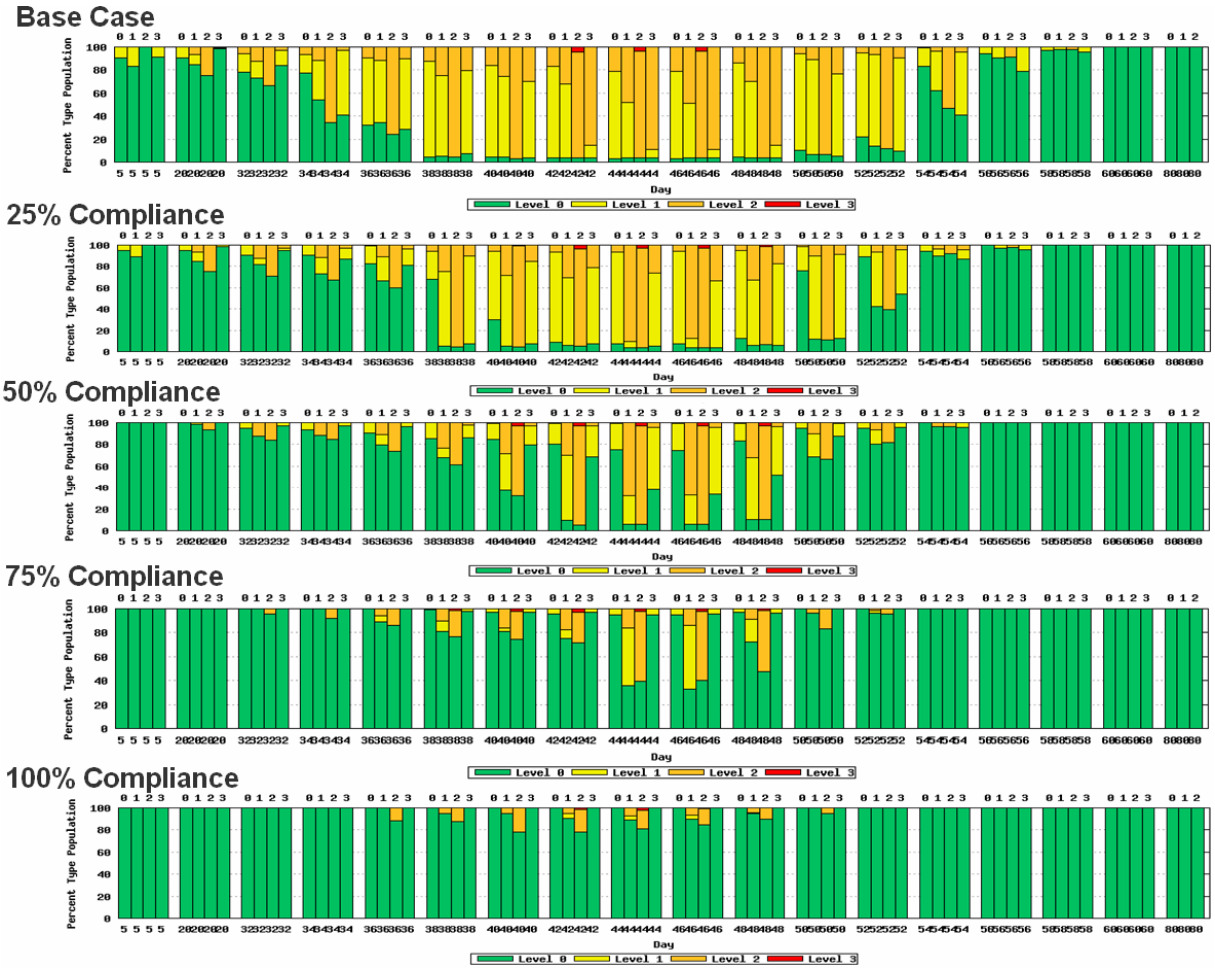


Figure 7.4-7 Best Practices with Varied Compliance in 40 Percent Absenteeism Scenario

7.4.4 Oversubscription

Network service providers engineer capacity based on the assumption that only a portion of users will be online at the same time. This allows network service providers to oversubscribe their capacity without any effect on performance during normal operation. Oversubscription ratios have been estimated to range from 10:1 to 100:1 [14, 15, 16]. This means that network service providers can offer full bandwidth to one-tenth to one-hundredth of their total subscriber population at once. If the traffic load increases beyond what the oversubscription ratio allows for, congestion will occur and users will experience degraded service in terms of decreased throughput. Oversubscription rates can vary based on anticipated subscriber growth, scheduled capacity upgrades, and other technology and business factors.

Without the detailed network architectures of individual network service providers, the Network component of the model was constructed from assumptions based on current engineering practices and open source information. The *Rocketfuel* traceroute data provided the topology of the service provider networks. However, last mile access architectures and individual link capacities are not included in the data set. The last mile access portion of the network was constructed based on market

research of typically deployed equipment and configurations. Link capacities in the last mile were selected using oversubscription estimates from industry analysis.

Since the oversubscription rate is an estimate and varies in real world implementation, several different oversubscription rates were examined in the model to analyze their effect on network performance. Figure 7.4-8 below shows the 40 percent absenteeism case with varied maximum oversubscription rates of 12:1, 25:1, and 42:1. The oversubscription rate in the model is unique to the population densities in each area served in the last mile, but is set to at a maximum of 12:1, 25:1, and 42:1.

As seen in the graphs, the oversubscription rate does have some effect on network congestion. In particular, decreasing the oversubscription rate decreases the length of the time of widespread congestion. However, the effect on reducing congestion during the peak of the pandemic is not very dramatic. The number of telecommuters (Type 1 and Type 2) experiencing Level 2 congestion during the peak of the pandemic only changes from around 80 percent for the 42:1 oversubscription rate to 70 percent for the 12:1 oversubscription rate. Thus, minor differences in oversubscription rates between network service providers is not anticipated to cause any provider to perform much better or worse than another provider during the peak of the pandemic. ***This result also suggests that targeted capacity upgrades that slightly lower the oversubscription rate may not enable the telecommuting strategy to succeed.***

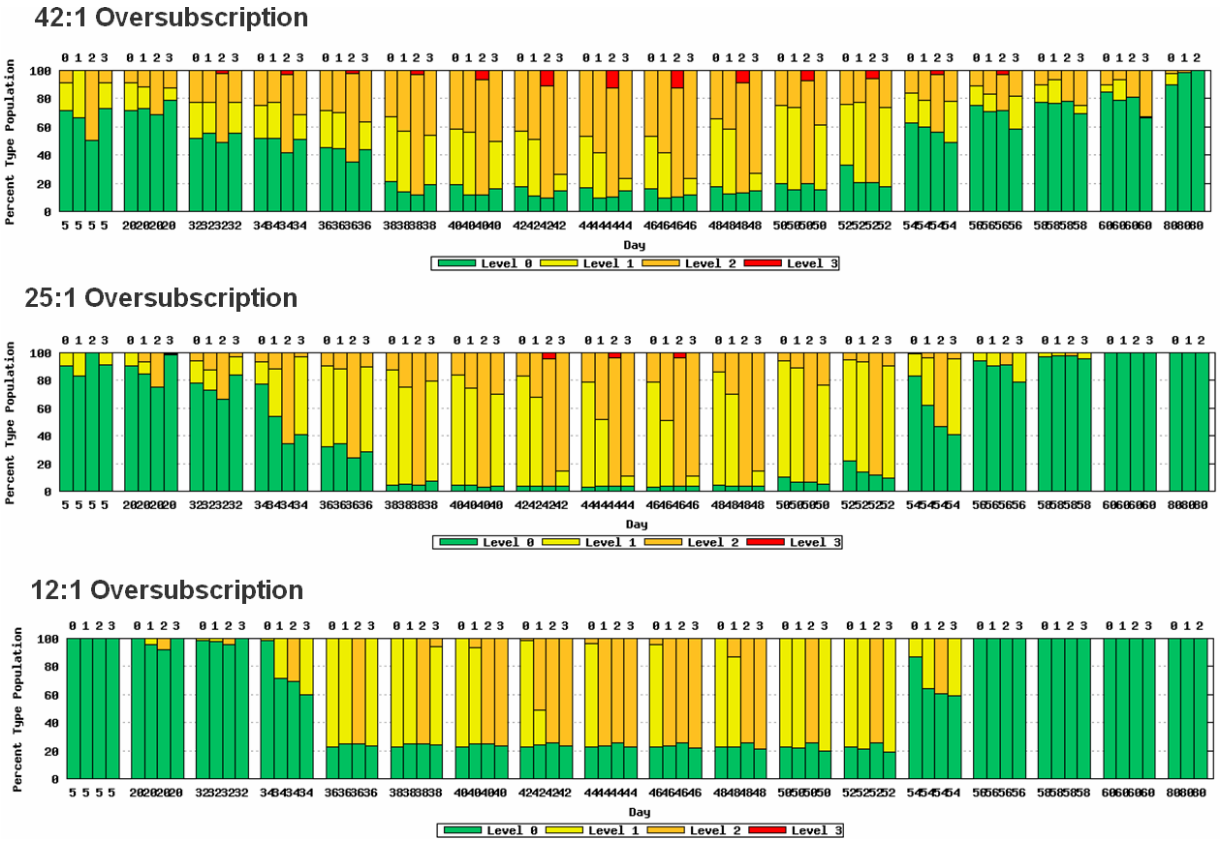


Figure 7.4-8 Oversubscription Rate in 40 Percent Absenteeism Scenario

8 Conclusions and Recommendations

In order to address the potential congestion points, phased preparations are proposed. In the short term, communications and IT best practices have been identified that can better prepare the telecommuting strategy to succeed. The communications and IT best practices are separated into four categories:

- **Enterprise Network Best Practices** – Guidance for businesses and government organizations on preparing enterprise IT infrastructures to support an anticipated increase in telecommuting traffic during a pandemic
- **Telecommuter Best Practices** – Guidance for business and government telecommuters on techniques to maintain business continuity while working from residential access networks
- **General Public Best Practices** – Guidance for the general public on voluntary actions to help reduce potential congestion in residential access networks
- **Network Service Provider Best Practices** – Guidance for network service providers on maintaining operations and existing service levels during a pandemic

In the long term, NGN Priority Services could potentially support business continuity during a pandemic by providing priority to critical telecommuter groups, if the required features are designed into the commercial communications infrastructure. Current priority communications services include GETS, WPS, and TSP. DHS NCS is working with the communications industry to migrate GETS and WPS into NGN architectures, as well as provide new priority services such as priority Internet access, video teleconferencing, and email. Initial capabilities of these services are not expected to be available until 2011-2012.

The model was used to quantify the impact of a pandemic on the communications infrastructure and assess the potential effect of communications and IT best practices on improving telecommuting performance. Some key findings from the model include:

- **Pandemic Parameters** – Pandemic disease parameters can significantly change the peak network user population.
- **Best Practices** – In many pandemic scenarios, high rate of compliance with all communications and IT best practices enables the telecommuting strategy to succeed. In particular, limiting video traffic appears to have a large impact.
- **Worst Case** – Potential pandemic scenarios exist that may lead to high network congestion. These include high absenteeism pandemic scenarios (i.e. large home network user population) and low compliance with the communications and IT best practices.

In order to better prepare for telecommuting during a pandemic influenza, the following actions are recommended:

- **Education and Outreach** – Identify outreach strategies to educate the government, industry, and general public on the communications and IT best practices. Compliance with the best practices may significantly improve the probability of the telecommuting strategy succeeding during a pandemic.
- **Worst Case Mechanisms** – Continue to work with industry to investigate mechanisms to implement when voluntary compliance with best practices is not enough to enable the telecommuting strategy to succeed.

Appendix A – Acronyms

PBX – Private Branch Exchange
CDC – Center for Disease Control
CMTS – Cable Modem Termination System
CS&C – Office of Cyber Security & Communications
DHS – Department of Homeland Security
DNS – Domain Name System
DSL – Digital Subscriber Line
DSLAM – Digital Subscriber Link Access Multiplexer
FBIIC – Financial and Banking Information Infrastructure Committee
FCC – Federal Communications Commission
FSSCC – Financial Services Sector Coordinating Council
GDP – Gross Domestic Product
GETS – Government Emergency Telecommunications Service
HHS – Department of Health and Human Services
HSC – Homeland Security Council
HSPD – Homeland Security Presidential Directive
IDS – Intrusion Detection System
IPS – Intrusion Prevention System
ISP – Internet Service Provider
IT – Information Technology
NCS – National Communications System
NGN – Next Generation Network
NIST – National Institute of Standards and Technology
NS/EP – National Security / Emergency Preparedness
P2P – Peer-to-Peer
PSTN – Public Switched Telephone Network
QoS – Quality of Service
ROSS – Rensselaer Optimistic Simulation System
SEIR – Susceptible-Exposed-Infected-Recovered
TSP – Telecommunications Service Priority
US-CERT – United States Computer Emergency Readiness Team
VOIP – Voice over Internet Protocol
VPN – Virtual Private Network
WPS – Wireless Priority Service

Appendix B – References

1. PandemicFlu.gov, "Frequent Questions", http://www.pandemicflu.gov/faq/pandemicinfluenza/2008.html
2. Secretary Michael Leavitt Speech at National Press Club in Washington D.C., 28 October 2005.
3. Congressional Budget Office. "A Potential Influenza Pandemic: Possible Macroeconomic Effects and Policy Issues," revised 27 July 2006.
4. Homeland Security Council *National Strategy for Pandemic Influenza Implementation Plan* May 2006, Department of Homeland Security *Pandemic Influenza Guide for Critical Infrastructure and Key Resources* June 2006, and Department of Health and Human Services *Community Strategy for Pandemic Influenza Mitigation* February 2007.
5. Bootsma, Martin and Ferguson, Neil. "The Effect of Public Health Measures on the 1918 Influenza Pandemic in U.S. Cities," Proceedings of the National Academy of Sciences, www.pnas.org/cgi/doi/10.1073/pnas.0611071104
6. Department of Health and Human Services *Community Strategy for Pandemic Influenza Mitigation* February 2007.
7. Homeland Security Council *National Strategy for Pandemic Influenza Implementation Plan* May 2006.
8. WorldatWork, "Telework Trendlines for 2006," February 2007.
9. World Economic Forum and Booz Allen Hamilton, "Influenza Pandemic Simulation," January 2006.
10. Sprint MPLS VPN IP Whitepaper, Revision 4.0, January 2005.
11. Kung, H.T. "Traffic Management for High-Speed Networks," Harvard University, National Academy Press, 1997.
12. DHS NCS "Pandemic Influenza Initial Assessment: Potential Impacts on Communications Networks," Working Draft, December 2005.
13. GAO "Characteristics and Choices of Internet Users," February 2001.
14. Grunwald, Dirk, et al. "Multimedia Quality of Service and Net Neutrality on Wireless Networks," University of Colorado at Boulder.
15. Greene, Tim. "DSL has a Secret," Network World, http://cnn.com/TECH/computing/9903/02/dslsecret.idg/
16. "Could High-Def Choke Internet," Associated Press, http://www.wired.com/techbiz/media/news/2006/05/70895
17. Pew Internet "Home Broadband Adoption 2006," May 28, 2006.
18. U.S. Census Bureau. "Characteristics of Children Under 18 Years by Age, Race, and Hispanic or Latino Origin, for the United States: 2000".
19. NCS Mission Statement, Executive Order 12472 as amended by E.O. 13286 Assignment of National Security and Emergency Preparedness Telecommunications Functions.

20. Ellacoya Networks, News Release, “Ellacoya Data Shows Web Traffic Overtakes Peer-to-Peer (P2P),” June 18, 2007.

21. Kermack, W. O and A. G. McKendrick (1927). “Contributions to the Mathematical Theory of Epidemics,” Proceedings *of the Royal Society*, Vol. 115A, pp. 700–721.

22. Bureau of Transportation Statistics, “The Intermodal Transportation Database,” http://www.transtats.bts.gov/

23. University of Washington, “Rocketfuel: An ISP Topology Mapping Engine,” http://www.cs.washington.edu/research/networking/rocketfuel

Appendix C – Pandemic Communications and IT Best Practices

C.1 Enterprise Networks Best Practices

This section provides guidance for businesses on preparing enterprise IT infrastructures to support an anticipated increase in telecommuting traffic during a pandemic influenza. These best practices address only communications and IT issues and should be part of an overall pandemic business continuity plan.

- Consider limiting remote access to only users critical to maintaining business continuity:
  Scaling enterprise networks to support all telecommuters during a pandemic may be cost prohibitive for some businesses. Businesses may alternatively consider limiting remote access during a pandemic to only users critical to maintaining business continuity. This may improve the performance of the critical users without significant investments in infrastructure.

- Consider limiting access to only business critical services through the enterprise connection:
  During a pandemic situation, increased telecommuting traffic and demand for remote access to many different services may put a strain on enterprise networks. In order to ensure high performance and availability, businesses may consider limiting access to only business critical services. Identifying which services are critical and which can be restricted should be part of a business continuity plan. At a minimum, businesses may consider restricting access to recreational content from the Internet through the enterprise connection. This may create bandwidth savings for critical telecommuting traffic.

- Consider adjusting or retiming automatic desktop backup software and software updates for telecommuters:
  Businesses should consider evaluating their policies and procedures for running desktop backup software and software updates. While these services are critical for data redundancy and keeping systems up to date for cyber security, these services can also be very bandwidth intensive. The high bandwidth demands of these services may pose a particular problem for telecommuters working from residential Internet access networks. Businesses may consider how these automatic services are delivered for telecommuters. For example, retiming these automatic services to occur during non-business overnight hours may enable telecommuters to obtain better performance during daytime business hours.

- Develop staffing contingency plans to maintain the enterprise networks and IT infrastructure with 40 percent absenteeism, to include support contractors. Cross-train staff as appropriate:
  The Homeland Security Council *National Strategy for Pandemic Influenza – Implementation Plan* advises businesses to plan under the assumption that up to 40 percent of staff may be absent for periods of about 2 weeks at the height of a pandemic wave. IT support likewise should plan to operate at this reduced staff level. This may be challenging as demands on enterprise networks from remote access connectivity are expected to increase at the same time that IT support staff levels decrease. Cross-training of IT staff may increase the resiliency of IT support.

- Consider procuring dedicated remote access tools for IT staff to access infrastructure and for Help Desk staff to provide technical support:
  During a pandemic situation, IT staff may need to access IT infrastructure remotely. Businesses should consider procuring dedicated support tools to allow IT staff to monitor, troubleshoot, and configure IT infrastructure from remote connections. These remote capabilities should be

provided with dedicated equipment to prevent these critical users from facing congestion. For example, a business could reserve ports on modem pools exclusively for IT staff as a backup method in case of congestion in VPN access.

Additionally, with an increased number of telecommuting employees, Help Desk technical support will be increasingly important during a pandemic. Businesses should also consider procuring dedicated remote access tools to enable Help Desk staff to provide technical support remotely.

- Consider obtaining Telecommunications Service Priority (TSP) for enterprises and Government Emergency Telecommunications Service (GETS) and/or Wireless Priority Service (WPS) capabilities for critical IT staff:
  TSP, GETS, and WPS are services provided through the Department of Homeland Security (DHS) National Communications System (NCS). TSP provides priority restoration and provisioning for users critical to coordinating and responding to a crisis. GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN) for voice and voice-band communications. WPS is the wireless equivalent to GETS and provides priority for calls from cellular telephones. Key Federal, state, local and tribal government, and critical infrastructure personnel are eligible for TSP, GETS, and WPS. Businesses supporting critical infrastructures, such as the power industry, should consider obtaining TSP for their enterprise and GETS and/or WPS for critical IT staff so these employees can support business continuity. More information about these services can be found at: http://gets.ncs.gov/, http://wps.ncs.gov/, and http://tsp.ncs.gov

- Evaluate Internet bandwidth:
  Businesses should evaluate Internet bandwidth requirements at enterprise gateway routers for a pandemic scenario. Existing bandwidth may not be adequate to support the increased telecommuting traffic anticipated during a pandemic. Businesses should assess their anticipated telecommuting demands during a pandemic and size their Internet bandwidth appropriately. Reviewing telecommuting traffic during winter storms or other scenarios in which the office was closed may provide insight into increases in telecommuting demand that may be seen during a pandemic.

- Investigate dual links from separate Internet providers to enterprise networks:
  During a pandemic, businesses may be heavily reliant on Internet connectivity to enterprise networks to maintain business continuity. In order to increase availability of the connection, businesses should investigate redundancy and diversity for their Internet connection. A dual Internet link provides redundancy and using separate Internet providers may increase diversity. When investigating a dual link, physical diversity should be examined as well.

- Assess ability to support increased teleconferencing demand. Consider adding audio/web conference ports:
  Anecdotal evidence from pandemic exercises and related winter storm situations indicates that teleconferencing demand could increase by several hundred percent during a pandemic. Businesses should assess their ability to support potential increased teleconferencing demand by working with the IT support staff or service provider who manages the teleconferencing services. Businesses should consider adding or contracting for additional audio/web conference ports to support the increased demand during a pandemic.

- Consider performing regular telecommuting exercises with employees to assess remote access capabilities and to familiarize employees with telecommuting policies and procedures:

A significant percentage of employees that telecommute during a pandemic may not be regular telecommuters. Businesses should take steps to ensure remote connectivity resources are in place on employee laptops and that employees are familiar with the policies and procedures associated with telecommuting. Businesses should also consider performing regular telecommuting exercises with employees. These exercises can help businesses better asses their remote access IT capabilities as well as provide an opportunity for employees to become more familiar with telecommuting policies and procedures.

- Provide multiple options for remote connectivity (e.g., Internet VPN, modem pool, iPass backup to modem pool, services that do not require VPN):
  Businesses should provide employees with multiple options for remote connectivity. Diversity of remote connectivity options can mitigate the effect of technical issues related to any one remote connectivity option. Telecommuters should be made aware of the remote connectivity options and should understand how network performance may be different with each technology.

- Assess critical supply chain with an assumption that foreign-produced materials and supplies will be curtailed and domestic supply chain will be degraded. Obtain onsite backup supplies:
  Businesses should assess the reliance of their IT infrastructure on domestic and international supply chains. During a pandemic, both domestic and international supply chains may be disrupted. Businesses should consider obtaining onsite backup supplies in order to sustain operations and handle equipment failures during a 6-8 week pandemic wave.

- Prepare to implement a restricted service model for computer maintenance/repair:
  Businesses should plan to continue to handle employee laptop issues during a pandemic. Technical support capabilities will likely be degraded due to the effect of the pandemic on IT support staff. Limiting physical contact with employees in order to decrease the spread of the pandemic will also complicate technical support. Business plans should include provisions for continued technical support with degraded capabilities while limiting disease spread.

- Implement cyber security best practices:
  Increased reliance on communications and IT services during a pandemic may increase an enterprise's cyber risk. With reduced support staff due to the pandemic, businesses may also have decreased capabilities to respond to cyber incidents. Businesses should evaluate their cyber-security posture and develop plans in advance. Each individual business will have different security requirements depending on the network configurations, applications and methods for access to the Internet. The cyber-security practices discussed here may not be adequate for all business situations. Cyber security best practices for enterprises collected from US Computer Emergency Response Team (US-CERT) include:
  - Have cyber security policies, plans, and procedures in place that set the vision, goals, and objectives for enterprise-wide cyber security – Policies, plans, and procedures that specifically address security of communications and IT systems and services should exist. These documents are the foundation for securing Enterprise Networks and are essential when preparing to operate under pandemic conditions.
  - Designate an individual to be responsible for the cyber security of enterprise IT infrastructure – By formally designating an individual to be responsible for cyber security, an enterprise can establish management support and priority for cyber security and provide direction, accountability, and oversight to cyber security.
  - Know if, where, and how internal systems and networks are connected to external networks – External network connections must be controlled in order to sufficiently manage vulnerabilities to an enterprise network and associated systems. Only by verifying

connectivity through the use of network tools designed for this purpose can systems managers be certain of the environment and security of their networks and systems.

- Use two-factor authentication when practical (See Homeland Security Presidential Directive/HSPD-12) – Two-factor authentication requires two authentication features (e.g., password, security token, biometric, etc.), thus increasing the access security of systems and networks by leveraging the concept of "something you have, something you know, and something you are."
- Require that all default passwords be changed – Most systems and applications are delivered and installed with a factory default password. Many of these default passwords are freely available on the Internet. If these defaults are not immediately changed, anyone who has ever installed an identical product or who can conduct moderate research, may have the ability to compromise the system.
- Use strong passwords or pass phrases and change them regularly (e.g., 30 – 90 days) – Strong passwords contain a mix of numbers, upper and lower case alphabetic, and special characters; and are not found in a dictionary. Pass phrases are the first letter of each word in a phrase used to construct a password, thus appearing to be a random selection of characters to the uninformed. It is important to find an appropriate balance between complexity and frequency of change, and the associated business needs and practicality. Passwords should be changed regularly to prevent them from being observed or guessed by unauthorized users.
- Actively maintain access control lists to ensure that all system and network accounts are modified, deleted, or de-activated as personnel leave or transfer into new roles – Upon termination, transfer, or other change in the role of an employee, an immediate review of their role and the access it requires should be undertaken. Employees who have been terminated should have all access (physical and electronic) revoked at once, thus closing a significant means of cyber attack, especially after adverse action terminations.
- Practice the concept of "least privilege" (i.e., users are only granted access to those files and applications based on roles and responsibilities) – The concept of "least privilege" means that people or systems are only granted as much access as they need to perform their assigned job function, and no more. A balance between what is good for security and what access is needed to allow business to be conducted smoothly is always the goal. Physical access to sensitive IT areas (e.g., IT server rooms, telecommunications closets, etc.) should always be restricted to those with a business need.
- Log cyber security events on firewalls and servers – Firewall and server logging is critical to an infrastructure's security. The logs should be configured to track potential security events (e.g., access attempts and dropped packets). Frequent review of log files plays a key role in ensuring that threats to system security are addressed promptly, stability is maintained, and systems are operating at maximum efficiency.
- Have defined IT Help Desk and CERT functions – A help desk is often the first line of defense to resolve most end-user issues. In the event of an emergency, having an established protocol and response team is critical to a timely response to the incident and an enterprise's ability to limit the extent and degree of the damage.
- Have an operational cyber incident response plan, which includes the maintenance of the IT helpdesk and computer emergency response functions – In addition to monitoring, incident response plans help provide a proactive approach to system incidents. Rather than waiting for them to occur and attempting to shape a response when time and resources are not at optimal levels, preparation ahead of time can greatly reduce the damage caused as well as the time to recover from an adverse event.
- Ensure current inventories of all internal and external network nodes – Maintaining a current inventory of cyber infrastructure nodes ensures that components can be located, tracked, diagnosed, and maintained effectively. Such nodes may include Internet and

wireless access points, VPNs, routers, firewalls, modems, vendor maintenance connections, private branch exchange (PBX) telephone systems, and alarm systems.

- Use cyber intrusion detection systems (IDS) or intrusion prevention systems (IPS) – An IDS will capture network or host traffic, analyze it for known attack patterns, and take specified action when it recognizes an intrusion or attempted intrusion. An IDS can either be network- or host-based. Network-based refers to an IDS that captures all network traffic, while host-based refers to an IDS installed on, and analyzes traffic for, a single device. IPS perform much the same function, but reside outside the network boundary.
- Perform periodic cyber vulnerability assessments – The vulnerabilities of critical systems and networks must be identified, evaluated for applicability to the operating environment, and then factored into a risk-management decision. Tools for the identification of vulnerabilities can take a number of forms, including a scanning tools to identify and report known vulnerabilities.
- Install and use up-to-date anti-virus programs – Viruses, worms, Trojans, and other malicious software code proliferate on the Internet and mutate on an unpredictable basis. Even without access to the Internet, malicious code can be introduced to an organization through actions (even unintended) of employees, support personnel, vendors, and business partners. Antivirus software should be required on every system in the organization whose architecture and application permit it. Daily scans are recommended during periods of increased risk.
- Scan e-mail attachments at the enterprise e-mail server – It is recommended that organizations use some level of filtering that will remove attachments with dangerous file extensions at the e-mail server as well as on individual computers. All major e-mail server applications provide some degree of filtering capabilities. If more filtering capability is desired, organizations may install third party applications that "plug in" to the e-mail server application and provide that additional functionality.
- Keep systems and applications software patched – A regular program of patching and updating helps ensure that new and existing vulnerabilities do not pose unacceptable risks to the organization. As new vulnerabilities are discovered in operating systems and software applications, patches and other updates are released to deal with them. Updating systems with these patches should be performed on a scheduled basis and should follow a documented procedure, and "auto update" options should be used when practical.
- Install, maintain, and use a firewall – An effective firewall policy restricts all access except that which is explicitly allowed (i.e., close everything and open only what you need) versus that which is explicitly restricted (i.e., close what you think of). Having a firewall that restricts communications to only those necessary for essential business is a key to limiting exposure. Maintaining a firewall is an ongoing responsibility to ensure that new vulnerabilities are accounted for. Firewalls that are "set and forget' can quickly become out of date.
- Use VPN or similar remote access technology when practical – VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends, and keep out traffic that is not properly encrypted.
- When using remote access technology provide guidance pertaining to rules of behavior – Many systems are connected in some fashion to other systems to share data and perform business functions. Rules governing these connections should be in place, especially when these connections are to components outside of the organization's direct control.
- Ensure that all employees receive cyber security awareness training commensurate with their responsibilities – Training should be refreshed and reinforced on a predetermined schedule and should be updated to reflect the changing threat and vulnerability environment. Training should also include policies, plans, and procedures that relate to telecommuting scenarios.

- Further information can be found at:
  - United States Computer Emergency Readiness Team (US-CERT) http://www.us-cert.gov/
  - National Institute of Standards and Technology (NIST) Computer Security Division http://csrc.nist.gov/publications/nistpubs/index.html

- Develop and maintain Business Continuity and Disaster Recovery (BC/DR) plans and procedures that address scenarios that include a dramatic increase in telecommuting staff:
  These plans should define operations of the enterprise in the event of a disaster and may include activation of an alternate computing facility or additional technological resources to mitigate risks associated with an increase in staff utilizing IT resources remotely. The plan should include the assurance of cyber security during contingency/recovery operations and specific roles and responsibilities for key personnel supporting the enterprise infrastructure.

C.2 Telecommuting Best Practices

This section provides guidance for business telecommuters on techniques to maintain business continuity while working from residential access networks.

- Review network service provider's Terms of Service to understand service expectations from residential Internet access:
  Businesses and employees that plan to rely on telecommuting during a pandemic should review and be familiar with the Terms of Service of their residential Internet service provider. The Terms of Service include important legal aspects of the service being offered including limitations on use of service, service availability, acceptable use policy, etc. Employees and business should understand the details and limitations on residential Internet access service when formulating their pandemic telecommuting plans.

- Consider working with communications service providers to obtain premium or dedicated service for critical employee groups:
  Businesses with truly critical telecommuting needs during a potential pandemic situation should consider working with network service providers to obtain premium or dedicated services for their critical employees. Examples of such services include private line, MPLS VPNs, and dedicated Internet access. A private line provides a dedicated circuit between the telecommuter's location and the enterprise network. A private line offers the highest level of service as the entire connection is dedicated and there are no shared resources. MPLS VPNs are similar to private lines but perform logical instead of physical separation. MPLS VPNs provide a managed service across the network service provider's core which provides the user with various Class of Service levels and performance and availability guarantees. MPLS VPNs can often be accessed by telecommuters through remote access technologies such as dial-up, DSL, and cable modem. However, connecting to the MPLS VPN in this way still requires going through local access aggregation points which may be subject to congestion. Dedicated Internet access provides a dedicated connection to the Internet. This can allow telecommuters to bypass potential local access congestion points. However, no end-to-end service level guarantees can be provided and other network congestion points may still affect telecommuter throughput.

  All of these services will cost more than traditional residential Internet access and may be cost prohibitive to some businesses. Actual costs will be determined by the type of service desired and the network provider's capabilities. The table below compares some potential premium service offerings for telecommuters.

Premium Service	Advantages	Disadvantages
Private Line	• Dedicated line between telecommuter and enterprise network eliminates any potential congestion points • Guaranteed service level from telecommuter to enterprise network	• Very high cost per telecommuter • Potential lack of route diversity
MPLS VPN	• Provides traffic separation and service level guarantees in network core	• High cost per telecommuter • Still subject to potential local access congestion points
Dedicated Internet Access	• Dedicated connection to Internet allows telecommuter to bypass potential local access congestion points	• High cost per telecommuter • Other network congestion points can affect telecommuter throughput

- Consider obtaining multiple connectivity options (e.g., DSL, cable modem, wireless broadband, satellite) for critical employee groups:
  Businesses with critical telecommuting needs during a potential pandemic should consider encouraging telecommuters to obtain multiple connectivity options. While increased communications traffic is expected across all communications technologies, variations in individual network provider architectures and unpredictable network user behavior during a pandemic may lead to different levels of performance. Telecommuters with multiple connectivity options can check these multiple options to find which services perform the best at which times.

- Consider obtaining Government Emergency Telecommunications Service (GETS) and/or Wireless Priority Service (WPS) capabilities for voice and low-speed data services for employees critical to business continuity:
  GETS and WPS are services provided through the Department of Homeland Security (DHS) National Communications System (NCS). GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN) for voice and voice-band communications. WPS is the wireless equivalent to GETS and provides priority for calls from cellular telephones. Key Federal, state, local and tribal government, and critical infrastructure personnel are eligible for GETS and WPS. Businesses in critical infrastructures should consider obtaining GETS and/or WPS for employees critical to business continuity so these employees have priority service for voice and voice-band data communications. More information about these services can be found at: http://gets.ncs.gov/ and http://wps.ncs.gov/.

- Consider performing large data transfers and backups during non-business overnight hours:
  Telecommuters should consider performing large data transfers and backups during non-business overnight hours. Telecommuters performing large data transfers during daytime business hours may find application performance degraded with increased communication traffic on the networks. These data transfer may perform better during non-business overnight hours. Avoiding these large data transfers during daytime business hours also reserves enterprise network resources for other telecommuters.

- Implement bandwidth saving practices (e.g., use compression techniques, convert frequently accessed corporate web pages to text-based):
  Businesses and telecommuters should consider implementing bandwidth saving practices. Bandwidth saving practices may help telecommuters run applications more efficiently during periods of increased communications traffic on public networks. For example, businesses could convert frequently accessed corporate webpages to text-based for use in a pandemic situation. This would enable telecommuters to download webpages faster and would reserve more network bandwidth for other users. Businesses should also consider implementing compression schemes to enable more efficient content delivery to telecommuters. Use of compression tools for large attachments, such as PowerPoint presentations, can significantly reduce file size and allow for faster and more efficient delivery.

- Consider implementing a staggered telework shift in order to prevent overloading of enterprise network capabilities:
  Businesses should consider implementing a staggered telework policy during a pandemic in order to prevent overloading enterprise network capabilities. Enterprise network resources may not be sized to accommodate the number of telecommuters that businesses may have during a pandemic. Businesses can implement a staggered telework policy in which critical users perform their functions during daytime business hours, while other non-critical users perform their functions

during nighttime hours. By implementing a staggered telework policy, businesses may be able to ensure enterprise networks will provide adequate performance to all users.

- Consider using Instant Messaging and two-way pager services in place of voice communications: Telecommuters should consider using Instant Messaging and two-way pager services as a substitute for bandwidth intensive voice communications in order increase their likelihood of communications and to reserve network resources for other users. Instant Messaging and two-way pagers provide communications services that use very low bandwidth and are very delay tolerant. During a pandemic with an anticipated increase in communications traffic, these communications services may perform better than high bandwidth and delay intolerant services.

- Limit the size of email attachments:
  Businesses and telecommuters should consider limiting the size of email attachments permissible. Large email attachments may create problems for email servers which are expected to be handling increased loads during a pandemic. Limiting large email attachments may prevent monopolization of email server resources and enable an increase in the total number of emails handled by the servers. Compression tools to reduce the size of email attachments should be used whenever possible.

- Log off enterprise network connections when not performing work that requires access to enterprise network (e.g., download email and then log off while reading and composing email): Telecommuters should log off their enterprise connection when they are not in use in order to conserve network resources for other users. Remaining connected to corporate VPN servers when not in use can prevent other users from connecting. For example, telecommuters should log on to enterprise networks to download email but log off while reading and composing email.

- Implement cyber security best practices for home computers:
  Increased numbers of employees working from home instead of the office during a pandemic also has cyber security implications. Employees normally protected by corporate firewalls must now rely on the security of their home networks. Telecommuters should follow cyber security procedures for their home networks from US-CERT including:
    - Install and use up-to-date anti-virus programs (daily scans are recommended during this increased risk period) – Viruses, worms, Trojans, and other malicious software code proliferate on the Internet and mutate on an unpredictable basis. Malicious code is so common that without automated protection it is a near certainty that systems will be infected. Antivirus software should be installed, used and regularly updated (i.e. daily) on every workstation in the home, especially those used for or connected to workstations used for telecommuting purposes.
    - Keep your system and applications software patched – As new vulnerabilities are discovered in operating systems and software applications, patches and other updates are released to deal with them. Updating systems with these patches should be done on a scheduled basis or as soon as possible following notification of the patches or updates.
    - Use care when reading e-mail with attachments and downloading/installing programs – With the prevalence of e-mail borne viruses and other spam messages that can include malicious software attachments, it is recommended that any suspicious e-mails received from unknown senders should remain unopened, be immediately deleted, and be reported to the organization's IT Help Desk. Likewise, downloading and installing of programs via the Internet should be done only from known and reliable sources.

The following practices are also recommended; however, employees should possess technical expertise and/or seek authorized help, when necessary, in implementing these practices. Note that these practices, alone, may not be adequate to protect the employee's computer in every situation but will contribute to reducing risk.

- Install and use a firewall – Ensure that it is properly configured and kept up to date - An effective firewall restricts all access except that which is explicitly allowed (i.e., close everything and open only what you need) versus that which is explicitly restricted (i.e., close what you think of). Having a firewall that restricts communications to only those necessary for essential applications is a key to limiting exposure. Maintaining a firewall is an ongoing responsibility to ensure that new vulnerabilities are accounted for. Firewalls that are "set and forget' can quickly become out of date.
- Utilize a robust password structure on home workstations – Use strong passwords or pass phrases and change them regularly (e.g., 30 – 90 days). Strong passwords contain a mix of numbers, upper and lower case alphabetic, and special characters; and are not found in a dictionary. Pass phrases are the first letter of each word in a phrase used to construct a password, thus appearing to be a random selection of characters to the uninformed. It is important to find an appropriate balance between complexity and frequency of change, and the associated business needs and practicality. Passwords should be changed regularly to prevent them from being observed or guessed by unauthorized users.
- Use two-factor authentication, when practical – Two-factor authentication utilizes two authentication features (e.g., password, security token, biometric, etc.), thus increasing the access security of systems and networks by leveraging the concept of "something you have, something you know, and something you are".
- Install and use a file encryption program for sensitive data – By encrypting files, you ensure that unauthorized people can't view data even if they can access it. When you use encryption, it is important to remember your passwords and passphrases; if you forget or lose them, you may lose your data.
- Establish physical access controls for the computer – If an intruder can gain physical access to a computer, he can bypass software-based access control mechanisms.
- Utilize and leverage the helpdesk and computer emergency response functions provided by the enterprise – A helpdesk is often the first line of defense to resolve most end-user issues. It provides a single point of contact, a tracking and resolution system, and staff that are available based on business needs (i.e., business hours only, 24/7, etc.). In the event of an emergency that might involve a system failure, a detected or active intrusion, or a virus attack, having an established protocol and response team is critical to a timely response to the incident and a company's ability to limit the extent and degree of the damage.

Further information can be found at the United States Computer Emergency Readiness Team (US-CERT) http://www.us-cert.gov/nav/nt01/

C.3 General Public Best Practices

This section provides guidance for the general public on voluntary actions to help reduce potential congestion residential access networks. In addition to identifying common best practices, it may be necessary to develop specific best practices that should be implemented for certain scenarios and in response to observed network performance thresholds.

- Voluntarily limit non-critical, recreational communications use:
  Network users in residential areas should limit their non-critical communications use including Internet access and wireline and wireless phone calls. Users are advised to keep communications traffic to a minimum and call times short to allow telecommuters and emergency services access to network resources. During a pandemic, increased telecommuting and demand for emergency services is expected to increase. Limiting non-critical, recreational communications usage reserves network resources for telecommuter applications and emergency services.

- Voluntarily limit streaming media, gaming, file transfer (e.g., P2P) and other bandwidth intensive communications services particularly during daytime business hours:
  Network users in residential areas should limit use of bandwidth intensive communications services, such as streaming media, gaming, and file transfer, particularly during daytime business hours in order to provide better performance for business telecommuting traffic. High bandwidth applications may cause congestion on residential Internet access networks and decrease performance for telecommuters. With increased telecommuters working from residential areas during a pandemic, attempts should be made to keep network resources available for business purposes.

- Consider configuring web browsers to block multimedia content (e.g., images, videos, sounds), see US-CERT "Securing Your Web Browser":
  Network users in residential areas should consider implementing bandwidth saving practices including configuring web browsers to block multimedia content. Blocking images, videos, and sounds from downloading may have significant bandwidth savings. With increased telecommuters working from residential areas during a pandemic, attempts should be made to keep bandwidth use as low are possible. Blocking multimedia content during a pandemic may also improve the security posture of the home network.

- Use broadcast news sources (e.g., television, radio) in place of online news sources when possible:
  Network users in residential areas should obtain information from broadcast sources whenever possible. Broadcast sources are "always on" and increased demand for content does not increase load on the networks. Use of broadcast information sources may make network resources available for the anticipated increase in telecommuters and emergency needs during a pandemic.

- Procure offline entertainment options to reduce network traffic during pandemic (e.g., desktop computer games, DVDs):
  Residents in given areas may be quarantined at home for an extended duration of time during a 6-8 week pandemic wave. During this time, the general public should be encouraged to use offline entertainment in place of online entertainment in order to reserve network resources for business uses. The general public should be prepared with offline entertainment options such as desktop video games and DVDs.

- Consider using Instant Messaging and two-way pager services in place of voice communications:

Network users in residential areas should consider using Instant Messaging and two-way pager services as a substitute for bandwidth intensive voice communications in order to reserve network resources for other users. Instant Messaging and two-way pagers provide communications services that use very low bandwidth. During a pandemic with anticipated increased communications traffic, these communications services may perform better than high bandwidth, delay intolerant services. Use of these low bandwidth services will also reserve network resources for other users.

- Limit the size of email attachments:
  Network users in residential areas should consider limiting the size of email attachments permissible. Large email attachments may provide issues for email servers who are expected to already be handling increased load during a pandemic. Limiting large email attachments may prevent monopolization of email server resources and enable an increase in the total number of emails handled by the servers. Compression tools to reduce the size of email attachments should be used whenever possible.

- Stagger online activity:
  Network users may be asked to voluntarily stagger online activity. For example, the specific time frames a user is allowed to go online could be based on whether user's street address is odd or even. Staggering online activity may reduce the peak traffic size and more evenly distribute traffic over time which could potentially improve telecommuter performance.

- Log off / shut down Internet connections when not in use:
  Network users in residential areas should log off or shut down Internet connections when they are not in use in order to conserve bandwidth and decrease cyber threats. Computers connected to the Internet may continue to put traffic demands on the network even when the user is not on the system. This traffic can come in the form of "keep-alive" messages or traffic from mal-ware unknowingly running on the computer. In order to avoid additional unnecessary traffic on the network and reserve network resources for others, network users should log off or shutdown Internet connections when not in use. Network users also remain immune from cyber attacks when their Internet connection is disabled.

C.4 Network Service Provider Best Practices

This section provides guidance for the network service providers on maintaining operations and existing service levels during a pandemic. Most network service providers have well established plans for maintaining and repairing service during emergency situations, ranging from individual fiber cuts to widespread damage of physical infrastructure by a natural disaster or terrorism. The network service provider best practices below are intended to illustrate some of the unique characteristics for network service providers of a pandemic situation in contrast to other emergencies. Many network service providers have developed pandemic plans and may already be taking many of these actions.

- Ensure customer services, including traditional voice calls, text messaging, teleconferencing, and data services are all designed to operate with minimal human intervention for a 6-8 week pandemic wave:
  Network service providers should ensure that services are designed to operate with minimal human intervention for at least a 6-8 week pandemic wave timeframe. Employee absenteeism and quarantines may limit worker mobility during a pandemic.

- Ensure network personnel have a secure remote access capability in order to reroute traffic around damaged network devices, interconnection problems or overutilized links:
  All industries, including network service providers, are expected to experience an impact to their workforce to the pandemic. In order to continue to operate with a degraded workforce, network service providers should ensure remote access capabilities to their network equipment are in place. These remote access capabilities will be critical in enabling network service providers to respond to other network issues that may arise during a pandemic.

- Ensure network technicians are able to use secure remote network management tools to quickly respond to physical and cyber events:
  In order to continue to operate with a degraded workforce during pandemic, network service providers should ensure that network management tools have remote access capabilities. Operations, maintenance, management, and provisioning functions will need to continue during a pandemic. Remote access capabilities may support these functions given a degraded workforce.

- Cross-train employees for critical roles as appropriate:
  The Homeland Security Council *National Strategy for Pandemic Influenza – Implementation Plan* advises businesses to plan under the assumption that up to 40 percent of staff may be absent for a period of about 2 weeks at the height of pandemic wave. Cross-training of staff may increase the resiliency of network service provider support.

- Examine ability of equipment inventories to meet customer demand during a 6-8 week pandemic wave:
  Network service providers should examine their ability to respond to changes in customer demand during a pandemic. A pandemic may cause a significant shift in the population toward spending more time at home. Increased demand for services on residential access networks may result. Network service providers should examine the ability of equipment inventories to respond to this anticipated change in customer demand. During a pandemic, both domestic and international supply chains may be disrupted. Businesses should consider obtaining onsite backup supplies in order to sustain operations and handle equipment failures during a 6-8 week pandemic wave.

- Obtain Government Emergency Telecommunications Service (GETS) and/or Wireless Priority Service (WPS) capabilities voice and low-speed data services for employees critical to business continuity:
  GETS and WPS are services provided through the Department of Homeland Security (DHS) National Communications System (NCS). GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN) for voice and voice-band communications. WPS is the wireless equivalent to GETS and provides priority for calls from cellular telephones. Key Federal, state, local and tribal government, and critical infrastructure personnel are eligible for GETS and WPS. Network service providers should consider obtaining GETS and/or WPS for employees critical to business continuity so these employees have priority service for voice and voice-band data communications. More information about these services can be found at: http://gets.ncs.gov/ and http://wps.ncs.gov/.

- Consider implementing rate limits or bandwidth caps in certain areas to improve traffic flow and reduce congestion:
  Network service providers should consider implementing rate limits or bandwidth caps in certain areas. Rate limits and bandwidth caps can be effective tools in improving traffic flow for all users. These tools may also be useful in limiting congestion to a certain area of the network. For example, a network service provider might rate limit a certain node so that a surge traffic load does not cause congestion to propagate to other parts of the network.