Department of Homeland Security

Pandemic Influenza Impact on Communications Networks Study

Communications and Information Technology Best Practices

October 2007

Executive Summary

The communications and information technology (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 an overall pandemic business continuity plans. The full list of Enterprise Network Best Practices is described in detail in Appendix A.

Remote user capabilities are a critical aspect of preparing enterprise networks for a pandemic situation. The Homeland Security Council (HSC) has advised businesses to plan for up to 40 percent of their employees to be absent during the 2 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 have increased reliance on communications and IT services to maintain business continuity during a pandemic. This increased reliance on communications and IT services can potentially 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 A.

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 A.

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 could 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 can enable them to perform functions more efficiently and also contribute less traffic to potential network congestion. Examples of bandwidth saving practices include performing large data transfers at night, logging off corporate virtual private network (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 A.

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 can potentially 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 videos online or children playing online games.

Limiting non-critical recreational traffic, particularly during day time work hours, will be key in 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 households 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 on 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 A 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 emergencies planned for 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 from an extended surge in traffic and degraded workforce. The surge in traffic will come primarily from increased telecommuters and 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 the ability of their inventories to support a potential 6-8 week disruption of supply chains.

Appendix A – Pandemic Communications and IT Best Practices

A.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.

A.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 managed 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. Managed 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
Managed 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/

A.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.

A.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.