# NRSC PANDEMIC CHECKLIST

Version 1
August 31, 2009

Prepared by the
Alliance for Telecommunications Industry Solutions (ATIS)
Network Reliability Steering Committee (NRSC)

ATIS is committed to providing leadership for, and the rapid development and promotion of, worldwide technical and operations standards for information, entertainment and communications technologies using a pragmatic, flexible and open approach. ATIS prioritizes the industry's most pressing, technical and operational issues, and creates interoperable, implementable, end to end solutions -- standards when the industry needs them and where they need them. Over 600 industry professionals from more than 250 communications companies actively participate in ATIS committees and incubator solutions programs.

The ATIS Network Reliability Steering Committee (NRSC)[1] was formed at the request of the first Network Reliability Council (NRC-1) to monitor network reliability. The NRSC strives to improve network reliability by providing timely consensus-based technical and operational expert guidance to all segments of the public communications industry.

As a trusted expert, the NRSC addresses network reliability improvement opportunities in an open, noncompetitive environment. The NRSC advises the communications industry through developing and issuing standards, technical requirements, technical reports, bulletins, best practices, and annual reports.

---

**Notice of Disclaimer & Limitation of Liability**

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

---

*Published by*
**Alliance for Telecommunications Industry Solutions**
**1200 G Street, NW, Suite 500**
**Washington, DC 20005**

Printed in the United States of America.

[1] This NRSC Subcommittee operates with the understanding that its guidance is distinct from other instruments; i.e. Best Practices are*not* standards *nor* regulations. Mandated implementation of the Best Practices is*inconsistent* with their intent. Rather, Best Practices are developed with the understanding that decisions regarding their applicability can only be made by individuals with sufficient competence and knowledge of relevant factors, including specific network implementations, technology, operational models and business considerations.

# CONTENTS

**Section 1: General**

**Section 2: Highly Relevant Voluntary Industy Best Practices**

**Best Practices Subcommittee Contributors**:

Rick Canaday, AT&T
John Garner, AT&T
Rick Griepentrog, AT&T
Percy Kimbrough, AT&T
Charles Oscarson, AT&T
Rick Krock, Bell Labs, Alcatel-Lucent
Karl Rauscher, Bell Labs, Alcatel-Lucent
Jim Runyon, Bell Labs, Alcatel-Lucent
Mark Peay, Cox Communications
Norris Smith, CenturyLink
Jim Stigliano, CenturyLink
Richard Cox, CenturyLink
Sharon Cary, MetroPCS
Stacy Hartman, Qwest
Lisa Siard, Sprint
Todd Tobis, Sprint
Becky Wormsley, Sprint
Richard Zinno, Sprint
Rose Fiala, T-Mobile
Harold Salters, T-Mobile
Gail Linnell, Telcordia
Spilios Makris, Telcordia
Mary Brown, Verizon
Robin Howard, Verizon
Dianne Tarpy, Verizon
Chris Oberg, Verizon Wireless

COMMUNICATIONS INFRASTRUCTURE

| | | | |
|---|---|---|---|
| Power | Software | Payload | Human |
| Environment | Hardware | Networks | Policy |

[1]

| PANDEMIC CHECKLIST ACTIVITY | | Environment | Hardware | Human | Networks | Payload | Policy | Power | Software |
|---|---|---|---|---|---|---|---|---|---|
| | **GENERAL** | | | | | | | | |
| | **Pandemic Related Links:** | | | | | | | | |
| | Department of Health and Human Services (HHS) | | | | | | | | |
| | http://www.pandemicflu.gov | | | | | | | | |
| | Community planning and mitigation information | | | | | | | | |
| | http://www.pandemicflu.gov/plan/community/commitigation.html | | | | | | | | |
| | Centers for Disease Control (CDC) | | | | | | | | |
| | www.cdc.gov/flu/avian | | | | | | | | |
| | Major news media | | | | | | | | |
| | Government contacts | | | | | | | | |
| | Local contacts (internal and external to company) | | | | | | | | |
| | World Health Organization (WHO) | | | | | | | | |
| | http://www.who.int/en | | | | | | | | |
| | | | | | | | | | |
| | **Attributes of a Pandemic:** | | | | | | | | |
| | Primary impact is on debilitation of workforce. | | | x | | | | | |
| | Impact on contractors/vendors and supply chain (e.g., more complicated process to transport spare hardware); particular concern from countries outside the United States. | | x | | | | x | | |
| | Pattern of traffic as employees access corporate networks from home. | | | x | x | x | | | |
| | Workforce fear (method of traveling between work and home, up to 40% of workforce impacted, which may affect family protection and care giving priorities). | | | x | | | | | |
| | Congestion from re-distribution of traffic (periphery and at enterprise access). | | | | x | x | | | |
| | Delayed response time to issues. | | | x | | | x | | |
| | Health of the network may deteriorate over time due to limited routine maintenance and outage response stemming from limited resources. | x | x | | | | | x | x |
| | Dramatically increased demand for broadband access. | | | | x | x | | | x |
| | Concerns of an infectious workplace. | x | | x | | | | | |
| | Limited resources (starts with people, then bandwidth, up and running systems, etc. ). | | x | x | x | x | | x | |
| | Limitations of service . . . prioritization of services. | | | | x | x | x | | |
| | Critical need for accurate information on the infection (corporate legal liability for providing advice) and other medical advice on inoculations, access to medical health. | | | x | | | x | | |
| | Increased need for access to emergency alert to community. | | | | x | x | | | |
| | Cycles, waves of infection (estimated 8 to 12 weeks); normal infection of flu ~2 weeks. | x | x | x | x | x | x | x | x |
| | Dislocation of population. | | | x | x | | | | |
| | Increase in VoIP access as workaround. | | | | x | x | | | |
| | Higher usage of Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS). | | x | | x | x | | | |

**PANDEMIC CHECKLIST ACTIVITY**

**COMMUNICATIONS INFRASTRUCTURE** [1]

| | | | |
|---|---|---|---|
| Power | Software | Payload | Human |
| Environment | Hardware | Networks | Policy |

| Best Practice | HIGHLY RELEVANT VOLUNTARY INDUSTRY BEST PRACTICES | Environment | Hardware | Human | Networks | Payload | Policy | Power | Software |
|---|---|---|---|---|---|---|---|---|---|
| 7-6-1038 | Network Operators, Service Providers and Equipment Suppliers should consider during times of disaster, communicating the disaster response status frequently and consistently to all appropriate employees - so that they all understand what processes have been put in place to support customers and what priorities have been established in the response. | | | x | | | | | |
| 7-6-5012 | Network Operators, Service Providers and Equipment Suppliers should limit access to areas of critical infrastructure to essential personnel. | x | | | | | x | | |
| 7-6-5165 | Network Operators, Service Providers and Equipment Suppliers should ensure that teleworkers (e.g., remote software developers) have the equipment and support necessary to secure their computing platforms and systems to the equivalent level of those on-site. Security software, firewalls and locked file cabinets are all considerations. | | | x | | | x | | x |
| 7-7-0491 | Network Operators, Service Providers and Equipment Suppliers should, where programs exist, coordinate with local, state and/or federal emergency management and law enforcement agencies for pre-credentialing to help facilitate access by technicians to restricted areas during an event. | x | | | | | x | | |
| 7-7-0609 | Network Operators and Service Providers should provide and maintain the contact information for mutual aid coordination for inclusion in mutual aid processes. | | | | | | x | | |
| 7-7-0804 | Service Providers should consider appropriate means for providing their customers with information about their traffic policies so that users may be informed when planning and utilizing their applications. | | | | | | x | | |
| 7-7-1023 | Network Operators, Service Providers and Equipment Suppliers should identify essential staff within their organizations that are critical to disaster recovery efforts. Planning should address the availability of these individuals and provide for backup staff. | | | x | | | x | | |
| 7-7-1026 | Network Operators and Service Providers should consider creating a corporate policy statement that defines a remote system access strategy, which may include a special process for disaster recovery. | | | | x | | x | | |
| 7-7-5028 | Network Operators, Service Providers and Equipment Suppliers should establish policies and procedures related to access control to provide exception access (e.g., emergency repair or response, forgotten credential, etc.). | x | | | | | x | | |
| 7-7-5062 | Network Operators, Service Providers and Equipment Suppliers should staff critical functions at appropriate levels, considering human factors such as workload and fatigue. | | | x | | | | | |
| 7-7-5126 | Network Operators, Service Providers and Equipment Suppliers should plan for contingency staffing to perform critical functions in response to crisis situations (e.g., natural disasters, labor strike, terrorist attack). | | | x | | | | | |
| 7-7-5134 | Network Operators, Service Providers and Equipment Suppliers should consider establishing a policy to manage the risks associated with key personnel traveling together. | | | x | | | | | |
| 7-7-5141 | Network Operators, Service Providers and Equipment Suppliers should consider restricting, supervising, and/or prohibiting tours of critical network facilities, systems and operations. | x | | x | | | x | | |
| 7-7-5160 | Network Operators, Service Providers, Equipment Suppliers and Property Managers should account for the possible absence of critical personnel in their business continuity plan. | | | x | | | | | |

| PANDEMIC CHECKLIST ACTIVITY | COMMUNICATIONS INFRASTRUCTURE<br>Power Software Payload Human<br>Environment Hardware Networks Policy<br>[1] | Environment | Hardware | Human | Networks | Payload | Policy | Power | Software |
|---|---|---|---|---|---|---|---|---|---|
| 7-7-5192 | Network Operators and Service Providers tenants of a telecom hotel should provide a current list of all persons authorized for access to the Property Manager, provide periodic updates to this list, and provide instructions for exceptions (e.g., emergency restoration personnel). | x | | | | | x | | |
| 7-7-5207 | Network Operators, Service Providers and Property Managers should take appropriate precautions to ensure that fuel supplies and alternate sources of power are available for critical installations in the event of major disruptions in a geographic area (e.g., hurricane, earthquake, pipeline disruption). Consider contingency contracts in advance with clear terms and conditions (e.g., Delivery time commitments, T&Cs). | x | | | | | | x | |
| 7-7-5226 | Network Operators, Service Providers and Property Managers should maintain liaison with local law enforcement, fire department, other utilities and other security and emergency agencies to ensure effective coordination for emergency response and restoration. | x | | | | | | | |
| 7-7-0476 | Network Operators and Property Managers should consider conducting physical site audits after a major event (e.g., weather, earthquake, auto wreck) to ensure the physical integrity and orientation of hardware has not been compromised. | | x | | | | | | |
| 7-7-5237 | Network Operators, Service Providers and Equipment Suppliers should verify the integrity of system spares and replenish utilized spares, as appropriate, as part of a disaster response at a facility. | | x | | | | | | |
| 7-6-0764 | Network Operators and Service Providers implementing protocols for the transport of VoIP data on IP networks should implement congestion control mechanisms such as those described by RFC 2309, RFC 2914, and RFC 3155. | | | | | | | | x |
| 7-7-0517 | Equipment Control Mechanisms: Equipment Suppliers should design network elements and associated network management elements with the combined capability to dynamically handle peak load and overload conditions gracefully and queue or shed traffic as necessary (e.g., flow control). | | | | | | | | x |
| 7-7-0588 | Network Operators, Service Providers and Equipment Suppliers should provide awareness training that stresses the services impact of network failure, the risks of various levels of threatening conditions and the roles components play in the overall architecture. Training should be provided for personnel involved in the direct operation, maintenance, provisioning, security and support of network elements. | x | x | x | x | x | | x | |
| 7-7-0658 | Network Operators, Service Providers and Property Managers should maintain adequate fuel on-site and have a well-defined re-supply plan. Generator life support systems (e.g., radiator fan, oil cooler fan, water transfer pumps, fuel pumps, engine start battery chargers) should be on the essential AC bus of the generator they serve. | | | | | | | x | |
| 7-P-0674 | **Smart Power Systems:** Network Operators, Service Providers and Property Managers should initiate or continue a modernization program to ensure that outdated power equipment is phased out of plant. They should consider the capabilities of smart controllers, local and remote monitoring, and alarm systems when updating their power equipment. Power monitors and smart controllers should be integrated into engineering and operational strategies. | | | | | | | x | |
| 7-7-1033 | Network Operators should develop a strategy for deployment of emergency mobile assets such as Cell on Wheels (COWs), cellular repeaters, Switch on Wheels (SOWs), transportable satellite terminals, microwave equipment, power generators, HVAC units, etc. for emergency use or service augmentation for planned events (e.g., National Special Security Event (NSSE)). | | x | | x | x | | x | |
| 7-7-5206 | Network Operators, Service Providers and Property Managers should maintain sufficient fuel supplies for emergency/backup power generators running at full load to allow for contracted refueling. | | | | | | | x | |
| 7-6-3203 | Service Providers should consider developing options that allow for call delivery from Emergency Notification Services to subscribers with call blocking/screening services in order to assist in the effectiveness of Emergency Notification Systems (Public Safety Mass Calling) and return calls from PSAPs. | | | | x | x | | | |
| 7-7-3210 | Emergency Operations Centers and PSAPs should consider obtaining connections to provide video (for viewing local weather and news information and monitoring distribution of information over EAS), and utilize that connection to provide diverse access to the Internet and telecommunications. | | | | x | x | | | |

| PANDEMIC CHECKLIST ACTIVITY | COMMUNICATIONS INFRASTRUCTURE<br>Power Software Payload Human<br>Environment Hardware Networks Policy<br>[1] | Environment | Hardware | Human | Networks | Payload | Policy | Power | Software |
|---|---|---|---|---|---|---|---|---|---|
| 7-7-5072 | Network Operators, Service Providers and Equipment Suppliers should perform risk assessments on key network facilities and control areas on a regular basis. Assessments should address natural disasters and unintentional or intentional acts of people on facility or nearby structures. | | | | x | x | | | |
| 7-7-5083 | Network Operators, Service Providers and Equipment Suppliers should maintain the availability of spares for critical network systems. | | | | x | x | | | |
| 7-7-5138 | Network Operators should plan for the possibility that impacted network nodes cannot be accessed by company personnel for an extended period of time and define the corporate response for restoration of service. | | | | x | x | | | |
| 7-7-5139 | Network Operators, Service Providers and Equipment Suppliers should consider establishing procedures for managing personnel who perform functions at disaster area sites. | | | | x | x | | | |
| 7-7-0416 | Capacity Management: Network Operators should design and implement procedures for traffic monitoring, trending and forecasting so that capacity management issues may be addressed. | | | | x | x | | | |
| 7-7-0419 | Capacity Management Systems: Service Providers should design and capacity-manage EMSs (Element Management Systems) and OSSs (Operational Support Systems) to accommodate changes in network element capacity. | | | | x | x | | | |
| 7-7-0518 | Capacity Monitoring: Network Operators should design and implement procedures for traffic monitoring, trending and forecasting so that capacity management issues may be understood. | | | | x | x | | | |
| 7-7-0574 | Network Operators and Service Providers should remotely monitor and manage the 911 network components using network management controls, where available, to quickly restore 911 service and provide priority repair during network failure events. | | | | x | x | | | |
| 7-7-0587 | Government, Network Operators and Service Providers of critical services to National Security and Emergency Preparedness (NS/EP) users should avail themselves of the Telecommunications Service Priority (TSP) program and support / promote as applicable. | | | | x | x | | | |
| 7-7-0595 | Network Operators and Service Providers should be aware of the dynamic nature of peak traffic periods and should consider scheduling potentially service-affecting procedures (e.g., maintenance, high risk procedures, growth activities) so as to minimize the impact on end-user services. | | | | x | x | | | |
| 7-P-0599 | **Crisis Event Simulation:** Network Operators and Service Providers should conduct exercises periodically to test a network's operational readiness for various types of events (e.g., hurricane, flood, nuclear, biological, and chemical), through planned drills or simulated exercises. The exercise should be as authentic as practical. Scripts should be prepared in advance and team members should play their roles as realistically as possible. | | | | x | x | | | |
| 7-7-0608 | Network Operators and Service Providers should utilize network surveillance and monitoring to keep overflow traffic conditions from adversely affecting networks. Interconnecting companies should address the control of overflow conditions in their bilateral agreements. | | | | x | x | | | |
| 7-7-0616 | Failure Effects Analysis: Network Operators should design and implement procedures to evaluate failure and emergency conditions affecting network capacity. | | | | x | x | | | |
| 7-7-1008 | Network Operators, Service Providers, and Equipment Suppliers should use the Incident Command System Standard for incident coordination and control in the emergency operations center and at the incident site. | | | | x | x | | | |

| PANDEMIC CHECKLIST ACTIVITY | COMMUNICATIONS INFRASTRUCTURE<br>Power \| Software \| Payload \| Human<br>Environment \| Hardware \| Networks \| Policy [1] | Environment | Hardware | Human | Networks | Payload | Policy | Power | Software |
|---|---|---|---|---|---|---|---|---|---|
| 7-7-1063 | Network Operators and Service Providers should set Initial Address Messages (IAMs) to congestion priority in accordance with applicable ANSI standards. This will ensure government emergency calls (e.g., 911, GETS ) receive proper priority during national emergency situations. Implementation in all networks should be in accordance with ANSI T1.111. | | | | x | x | | | |
| **Best Practice** | **PROPOSED NRSC PANDEMIC BEST PRACTICES** | | | | | | | | |
| 7-P-0785 | **Network Operation Center (NOC) Communications Remote Access**: Network Operators and Service Providers should consider the need for remote access to critical network management systems for network management personnel working from distributed locations (e.g., back-up facility, home) in the event of a situation where the NOC cannot be staffed (e.g., pandemic). | | x | | | x | | | |
| 7-P-0786 | **Remote Access for Technical Support:** Network Operators and Service Providers should consider allowing equipment suppliers or 3rd party service providers remote secured access to vital hardware components in order to provide real-time feedback and suggestions on device enhancements and performance during a crisis (e.g., reroute traffic during overload). | | | x | x | x | | | |
| 7-P-0787 | **Back-Up Power Fuel Supply:** Network Operators, Service Providers and Property Managers, where feasible, should consider the use of fixed alternate fuel generators (e.g., natural gas) connected to public utility supplies to reduce the strain on refueling. | | | | | | x | x | |
| 7-P-0789 | **Travel Guidelines**: Network Operators, Service Providers, and Equipment Suppliers should consider modifying travel guidelines for use during a pandemic or other appropriate crisis situation. | | | x | | | | | |
| 7-P-0790 | **Personal Protective Equipment**: Network Operators, Service Providers, and Equipment Suppliers should consider providing personal protective equipment barriers to infection (e.g., masks, disposable gloves, and sanitizers) in locations where multiple employees are located. | x | | x | | | | | |
| 7-P-0791 | **Protective Equipment Training:** Network Operators, Service Providers, and Equipment Suppliers should consider providing appropriate personnel training in the use of personal protective equipment specific to a pandemic or other appropriate crisis situation and the employee's particular job. | x | | x | | | | | |
| 7-P-0792 | **Attendance Guidelines:** Network Operators, Service Providers, and Equipment Suppliers should consider modifying attendance guidelines for use during a pandemic, or other appropriate events. | | | x | | | | | |
| 7-P-0793 | **Telecommuting:** Network Operators, Service Providers, and Equipment Suppliers should, as part of business continuity planning, identify employees that can perform their tasks from home and consider provisions for allowing them to do so. | | | x | | | | | |
| 7-P-0794 | **Telecommuting Infrastructure:** Network Operators, Service Providers, and Equipment Suppliers should consider sizing their remote access capabilities for employees to accommodate increased usage during a pandemic, or other crisis situations. | | | x | x | | | | |
| 7-P-0795 | **Virtual Collaboration:** Network Operators, Service Providers, and Equipment Suppliers should consider utilizing virtual collaboration and remote meetings during a pandemic or other crisis situations by providing remote services and size these services to accommodate the anticipated load. | | | x | x | | | | |
| 7-P-0796 | **Deferral of Operations Activities:** Network Operators, Service Providers, and Equipment Suppliers should consider developing guidelines for the deferral of specific maintenance or provisioning activities during certain situations (e.g., pandemic, holiday, National Special Security Event). | | | x | | | x | | |
| 7-P-0797 | **Workforce Augmentation:** Network Operators, Service Providers, and Equipment Suppliers should consider plans for augmenting the existing workforce from outside of the affected area during a pandemic or other crisis situation. | | | x | | | x | | |
| 7-P-0798 | **Transportation Delay Contingencies:** Network Operators, Service Providers and Equipment Suppliers should give consideration to alternate modes of transportation, the availability of spares and how to effectively distribute personal protective equipment, in order to be prepared for situations where transportation of materials may be delayed (e.g., pandemic, other crisis situation). | | x | | | | x | | |

[1] Rauscher, Karl. F., *Protecting Communications Infrastructure* , Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004; Proceedings of 2001 IEEE Communications Society Technical Committee Communications Quality & Reliability (CQR) International Workshop, www.comsoc.org/~cqr; ATIS-0100523.2007, *ATIS Telecom Glossary 2007* , < http://www.atis.org/glossary/definition.aspx?id=8347 >

## Communications Infrastructure Ingredient Definitions [1]

**Environment** - Environment includes a wide range of areas such as buildings, tower sites, satellite glide paths, cable trenches, ocean floors and overhead lines. Communications infrastructure is virtually everywhere.

**Hardware** - The hardware area includes the broad category of physical electronics and related components that are part of communications systems.

**Human** - This area includes employees of network operators, carriers, equipment suppliers, government, and property managers who are associated with the development, deployment and management of public data network communications systems.

**Networks** - Network is defined as a series of points or nodes interconnected by Communication paths. Networks can interconnect with other networks and contain sub-networks.

**Payload** - Payload includes any messages that go across networks.

**Policy** - The policy area includes agreements between multiple parties covering issues such as industry standards and practices, along with physical and logical interfaces (e.g., protocols).

**Power** - Power area includes the internal power systems, batteries, grounding, high voltage and other cabling, fuses, back-up emergency generators and fuel.

**Software** - The software area includes the broad category of operating systems, applications, and firmware that are part of a communications system.