



ATIS STANDARD

ATIS-0100018

ATIS Standard on -

**NRSC PANDEMIC CHECKLIST**



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 250 companies actively formulate standards in ATIS' 18 Committees, covering issues including: IPTV, Service Oriented Networks, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, and Billing and Operational Support. In addition, numerous Incubators, Focus and Exploratory Groups address emerging industry priorities including "Green", IP Downloadable Security, Next Generation Carrier Interconnect, IPv6 and Convergence.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, please visit < <http://www.atis.org> >.

---

The ATIS Network Reliability Steering Committee (NRSC)<sup>1</sup> 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.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith.
--

---

### ATIS-0100018 NRSC Pandemic Checklist

Is an ATIS Standard developed by the ATIS NRSC

*Published by*

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

Copyright © 2010 by Alliance for Telecommunications Industry Solutions  
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

---

<sup>1</sup> 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.



# **NRSC PANDEMIC CHECKLIST**

**Version 1  
August 31, 2009**

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

# CONTENTS

- Section 1: General**
  - Monitoring Pandemic..... 6
  - Communications Infrastructure Definitions..... 6
  - Attributes of a Pandemic..... 6
- Section 2: Highly Relevant Voluntary Industry Best Practices**
  - Current Best Practices..... 7
  - Proposed Pandemic Best Practices..... 10



**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



PANDEMIC CHECKLIST ACTIVITY

COMMUNICATIONS INFRASTRUCTURE

Power	Software	Payload	Human
Environment	Hardware	Networks	Policy

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

Best Practice	HIGHLY RELEVANT VOLUNTARY INDUSTRY BEST PRACTICES						
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				



**COMMUNICATIONS INFRASTRUCTURE**

Power	Software	Payload	Human
Environment	Hardware	Networks	Policy

**PANDEMIC CHECKLIST ACTIVITY**

		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	<b>Crisis Event Simulation:</b> 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				Environment	Hardware	Human	Networks	Payload	Policy	Power	Software
		Power	Software	Payload	Human								
Best Practice		Environment	Hardware	Networks	Policy								
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				
<b>PROPOSED NRSC PANDEMIC BEST PRACTICES</b>													
7-P-0785	<b>Network Operation Center (NOC) Communications Remote Access:</b> 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	<b>Remote Access for Technical Support:</b> 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	<b>Back-Up Power Fuel Supply:</b> 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	<b>Travel Guidelines:</b> 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	<b>Personal Protective Equipment:</b> 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	<b>Protective Equipment Training:</b> 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	<b>Attendance Guidelines:</b> 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	<b>Telecommuting:</b> 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	<b>Telecommuting Infrastructure:</b> 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	<b>Virtual Collaboration:</b> 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	<b>Deferral of Operations Activities:</b> 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	<b>Workforce Augmentation:</b> 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	<b>Transportation Delay Contingencies:</b> 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		

<sup>1</sup> 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](http://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.