ATIS-0100018

ATIS Standard on -

NETWORK RELIABILITY STEERING COMMITTEE (NRSC)

PANDEMIC CHECKLIST

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

ATIS-0100018, *Network Reliability Steering Committee (NRSC) Pandemic Checklist*

Is an ATIS Standard developed by the **ATIS Network Reliability Steering Committee (NRSC)**.

Published by

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

ATIS-0100018

ATIS Standard on

Network Reliability Steering Committee (NRSC) Pandemic Checklist, Version 2

Alliance for Telecommunications Industry Solutions

Approved February 23, 2015

Abstract

The NRSC compiled a checklist of voluntary industry Best Practices and relevant links as a reference in preparation for a pandemic event.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Network Reliability Steering Committee (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.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, NRSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, Network Reliability Steering Committee (NRSC), which was responsible for its development, had the following leadership:

S. Hartman, NRSC Co-Chair (CenturyLink)

R. Krock, NRSC Co-Chair and Best Practices Subcommittee Co-Chair (Alcatel-Lucent)

R. Howard, NRSC Best Practices Subcommittee Co-Chair (Verizon)

The **Best Practices** Subcommittee was responsible for the development of this document.

CONTENTS

PANDEMIC CHECKLIST ACTIVITY	COMMUNICATIONS INFRASTRUCTURE [1]	Environment	Hardware	Human	Networks	Payload	Policy	Power	Software
	Power / Software / Payload / Human / Environment / Hardware / Networks / Policy								
	GENERAL								
	Pandemic Related Links:								
	Department of Health and Human Services (HHS)								
	http://www.pandemicflu.gov								
	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	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	x		

PANDEMIC CHECKLIST ACTIVITY	COMMUNICATIONS INFRASTRUCTURE: Power, Software, Payload, Human, Environment, Hardware, Networks, Policy [1]	Environment	Hardware	Human	Networks	Payload	Policy	Power	Software
Best Practice	**HIGHLY RELEVANT VOLUNTARY INDUSTRY BEST PRACTICES**								
9-9-1038	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider during all hazard and preplanned events, communicating the response status frequently and consistently to all appropriate employees detailing what processes have been put in place to support customers and what priorities have been established in the response.			x					
9-9-5012	Network Operators, Service Providers, Public Safety and Equipment Suppliers should limit access to areas of critical infrastructure to essential personnel.	x					x		
9-6-5165	Network Operators, Service Providers and Equipment Suppliers should ensure that teleworkers have the equipment and support necessary to secure their computing platforms and systems at an equivalent level of those within company office facilities (e.g., Security software, firewalls and secure documents storage).			x			x		
9-7-0491	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		
9-7-0609	Network Operators and Service Providers should provide and maintain the contact information for mutual aid coordination for inclusion in mutual aid processes.						x		
9-7-0804	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		
9-9-1023	Network Operators, Service Providers, Public Safety 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		
9-9-1026	Network Operators, Public Safety and Service Providers should consider creating a policy statement that defines a remote system access strategy, which may include a special process for disaster recovery.				x		x		
9-7-5062	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should staff critical functions at appropriate levels, considering human factors such as workload and fatigue.			x					
9-7-5134	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider establishing a policy to manage the risks associated with key personnel traveling together.			x					
9-7-5141	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider restricting, supervising, and/or prohibiting tours of critical network facilities, systems and operations.	x		x			x		
9-9-5160	Public Safety, Network Operators, Service Providers, Equipment Suppliers and Property Managers should have contingency plans in place for the possible absence of critical personnel in their business continuity plan.			x					
9-7-5192	Network Operators and Service Providers that are 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		
9-9-5207	Network Operators, Service Providers, Public Safety 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	

PANDEMIC CHECKLIST ACTIVITY	COMMUNICATIONS INFRASTRUCTURE [1]	Environment	Hardware	Human	Networks	Payload	Policy	Power	Software
9-7-5226	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		x					
9-9-0476	Network Operators, Public Safety, 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	x						
9-9-5237	Network Operators, Service Providers, Pubic Safety and Equipment Suppliers should verify the integrity of system spares and replenish spares, as appropriate, as part of a disaster response and at the conclusion of a disaster response at a facility.		x						
9-6-0764	Network Operators and Service Providers should implement congestion control mechanisms for transporting VoIP data on IP networks.								x
9-7-0517	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
9-9-0658	Network Operators, Service Providers, Property Managers and Public Safety should ensure generator life support systems (e.g., radiator fan, oil cooler fan, water transfer pumps, fuel pumps, engine start battery chargers) are on the essential Alternating Current (AC) buss of the generator they serve.							x	
9-9-0674	Network Operators, Service Providers, Property Managers, and Public Safety should initiate or continue a modernization program to ensure that outdated power equipment is phased out of plant considering capabilities of smart controllers, local and remote monitoring and control, alarm systems when updating power equipment, and being integrated into engineering and operational strategies.							x	
9-9-1033	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	
9-9-5206	Network Operators, Service Providers, Public Safety and Property Managers should maintain sufficient fuel supplies for emergency/backup power generators running at full load and ensure contracted refueling is in place.							x	
9-6-3203	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			
9-7-5072	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should perform risk assessments on key network facilities and control areas on a regular basis, taking into account natural disasters and unintentional or intentional acts of people impacting the facility or nearby structures.	x			x	x			
9-7-5083	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should maintain the availability of spares for critical network systems.		x		x				
9-7-5138	Network Operators and Public Safety 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				
9-9-5139	Network Operators, Service Providers, Public Safety and Equipment Suppliers should consider establishing procedures for managing personnel who perform functions at disaster area sites.			x		x			

PANDEMIC CHECKLIST ACTIVITY	COMMUNICATIONS INFRASTRUCTURE: Power, Software, Payload, Human, Environment, Hardware, Networks, Policy [1]	Environment	Hardware	Human	Networks	Payload	Policy	Power	Software
9-9-0416	Network Operators, Service Providers, and Public Safety should design and implement procedures for traffic monitoring, trending and forecasting so that capacity management issues may be addressed.				x	x			
9-7-0419	Network Operators and 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			x
9-9-0574	Network Operators, Service Providers, and Public Safety should actively monitor and manage the 9-1-1 network components using network management controls, where available, to quickly restore 9-1-1 service and provide priority repair during network failure events. When multiple interconnecting providers and vendors are involved, they will need to cooperate to provide end-to-end analysis of complex call-handling problems.				x	x	x		
9-9-0587	Government, Network Operators and Service Providers of critical services to National Security and Emergency Preparedness (NS/EP) users should be familiar with the Telecommunications Service Priority (TSP) program and support / promote it as applicable.				x	x	x		
9-9-0595	Network Operators, Service Providers, and Public Safety 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			
9-9-0599	Network Operators, Service Providers, and Public Safety 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, simulated exercises being as authentic as practical including scripts prepared in advance with team members playing their roles as realistically as possible.			x	x				
9-9-0608	Network Operators and Service Providers should utilize network surveillance and monitoring to keep overflow traffic conditions from adversely affecting networks.				x	x			
9-9-0616	Network Operators and Service Providers should design and implement procedures to evaluate failure and emergency conditions affecting network capacity.				x	x			
9-7-1008	Network Operators, Service Providers, and Equipment Suppliers should use the Incident Command System for incident coordination and control in the emergency operations center and at the incident site.				x		x		
9-9-1063	Network Operators, Public Safety 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., 9-1-1, GETS) receive proper priority during national emergency situations. Implementation in all networks should be in accordance with ANSI T1.111.				x	x	x		
9-8-0785	Network Operators and Service Providers should consider secured 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		x
9-9-0786	Network Operators, Service Providers, and Public Safety should consider allowing Equipment Suppliers or third party Service Providers remote secured access to vital hardware components.		x	x	x				x
9-8-0787	Network Operators, Service Providers, and Property Managers 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	
9-8-0789	Network Operators, Service Providers, and Equipment Suppliers should consider modifying travel guidelines/policies for use during a pandemic or other crisis situations.			x					

PANDEMIC CHECKLIST ACTIVITY	COMMUNICATIONS INFRASTRUCTURE [1]	Environment	Hardware	Human	Networks	Payload	Policy	Power	Software
	Power / Software / Payload / Human / Environment / Hardware / Networks / Policy								
9-8-0790	Personal Protective Equipment: Network Operators, Service Providers, Equipment Suppliers and Public Safety should consider providing personal protective equipment (PPE) for infection control (e.g., masks, disposable gloves, and sanitizers) in locations where multiple employees are located.	x		x					
9-8-0791	Network Operators, Service Providers, Equipment Suppliers, Government, and Public Safety should consider providing personnel training in the use of personal protective equipment (PPE) specific to a pandemic or other crisis situations and the employee's particular job.			x					
9-8-0792	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider modifying attendance guidelines during a pandemic, or other crisis situations.			x					
9-8-0793	Network Operators, Service Providers, and Equipment Suppliers should, as part of business continuity planning, identify employees that can perform their tasks from alternate locations and consider provisions for enabling them to do so.			x			x		
9-8-0794	Network Operators, Service Providers, and Equipment Suppliers should, as part of business continuity planning, provide for elevated /increased utilization of remote access capabilities for telecommuting purposes by employees during a pandemic, or other crisis situations.			x	x				
9-8-0795	Network Operators, Service Providers, and Equipment Suppliers should as part of business continuity planning, plan for elevated/increased utilization of virtual collaboration and remote meetings capabilities during pandemics or other crisis situations.			x	x		x		
9-8-0796	Network Operators, Service Providers, and Equipment Suppliers should, as part of business continuity planning, 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		
9-9-0797	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider creating a workforce augmentation plan prior to a pandemic or other crisis situation.			x			x		
9-8-0798	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider, as part of business continuity/disaster recovery, alternate transportation and delivery methods for equipment, spares, and personal protective equipment to prepare for situations where transportation and delivery may be delayed (e.g., pandemic, other crisis situations).		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.