8. Communication and Information Sector

8.1. Introduction

Communication and information systems have become increasingly critical parts of our daily lives. For example, the banking system relies on the internet for financial transactions, documents are transferred via internet between businesses and e-mail is a primary means of communication between and within companies. When the internet is not available, commerce is directly affected and economic output is reduced.

Communication and information systems have seen incredible continual development and use over the past 20-30 years. In terms of system types, functionality, and speed, some of the most notable changes of communication and information systems over the past few decades have been:

- Moving from a society that relies on fixed line (i.e., land line) telephones as the primary means of two-way voice communication to one that relies heavily on mobile devices (i.e., cell phones) and internet (Voice over Internet Protocol, VoIP) for voice communication, text messages and email. Many now have abandoned traditional land lines in favor of mobile phones and VoIP.
- Moving from a society where large personal computers were used to communicate via email and access information via the internet to a society where smaller mobile devices, such as laptops and cell phones, are used, constantly, for the same purpose.
- Increased use of mobile devices and higher technology for one-way communication (i.e., receiving information) have become used increasingly in place of more traditional methods, such as television and radio. More and more people now use their laptops, smart phones and tablets to read news on the internet, watch movies and television shows, instead of using traditional methods such as television.
- More recently, social-networking sites have begun to be used by businesses for collaboration, marketing, recruiting, etc.

As in many other developed countries, most people in the United States take these services for granted until they are unavailable. Unfortunately, it is often the case that communication and information systems are lost in the wake of natural disasters – a time when they are needed most for:

1. Relaying emergency and safety information to the public.
2. Coordinating recovery plans among first responders and community leaders.
3. Communication between family members and loved ones to check on each other's safety.
4. Communication between civilians and emergency responders.
5. Communication between emergency responders in the field.

This chapter addresses disaster resilience of communication and information systems. The first steps for a community to address resilience of their infrastructure are to identify the regulatory bodies, parties responsible for condition and maintenance of the infrastructure, work with the stakeholders to determine the performance goals of the infrastructure, evaluate the state of the existing communication and

information infrastructure systems, identify the weak links in the infrastructure network and prioritize upgrades to improve resilience of the network. This chapter identifies a tool that can be used by communities to set their performance goals for various hazards, stakeholders/owners of the various components of communications infrastructure, discusses critical infrastructure of various communication and information systems, and recommends improvements that can be made to enhance the resilience of the system.

8.2. Performance Goals

Although the goal of communities, infrastructure owners, and businesses is to have continued operation at all times, it is unlikely that this will be the case in the wake of all disaster events. Depending on the magnitude and type of event, the levels of damage and functionality will vary. Most importantly, performance goals of communications infrastructure will vary from community-to-community based upon its needs and should be defined by the community and its stakeholders. This section provides an example of performance goals that communication infrastructure stakeholders and communities can use to assess their infrastructure and take steps in improving their resilience to disaster events. Before we can establish the performance goals, it is imperative to understand who the owners, regulatory bodies and stakeholders of the communications infrastructure are because they should all be involved in establishing the performance goals and working together to narrow the gaps in resilience.

Ownership and regulation of communication and information infrastructure systems adds a layer of complexity for resilience. Governments typically do not own communication infrastructure other than in their own facilities. However, Federal, State and Local government agencies are involved in the regulation of communications infrastructure. The Federal Communications Commission (FCC) has a Communications Security, Reliability, and Interoperability Council that promotes best practices for resiliency, but there is no requirement for compliance with the standards. The FCC has authority over wireless, long-distance telephone, and internet services, whereas state agencies have authority over local landlines and agencies at all levels have regulatory authority over cable (City of New York 2013). Within these three levels of government, there may be multiple agencies that are involved in overseeing infrastructure. State and local Departments of Transportation (DOTs) control access to roadway rights-of-way for construction. The local Department of Buildings (DOB) regulates the placement of electrical equipment, standby power, and fuel storage at critical telecommunications facilities as specified in their local Building Codes (City of New York 2013).

Service providers own communications infrastructure. The Telecommunications Act of 1996 was established to promote competition in the communications industry (FCC 2011), which would result in lower prices for customers. This has resulted in a growing number of industry players who share infrastructure to offer options for their services to customers more efficiently. Telecommunication and Internet Service Providers, such as AT&T and Verizon, often also share infrastructure (e.g., utility poles for overhead wires) with providers in the energy industry. It is, therefore, essential that key members from these service providers are involved in establishing, or agreeing to, the performance goals for the communications infrastructure. Improved performance of their infrastructure, much like the power industry, will result in improved service in the wake of a disaster event. A service provider may benefit from excellent performance following a disaster event because customers frustrated with their own service may look for other options that are more reliable.

After the AT&T divestiture of 1984, the end-user became responsible for the voice and data cabling on its premises (Anixter Inc. 2013). Therefore, building owners are responsible for communications infrastructure within their facilities. As a result, standards have been developed by the American National Standards Institute/Telecommunications Industry Association (ANSI/TIA) for different types of premises, including:

- Commercial buildings (e.g., office and university campus buildings);
- Residential buildings (e.g, single and multi-unit homes);
- Industrial buildings (e.g., factories and testing laboratories); and
- Healthcare facilities (e.g., hospitals).

Communications infrastructure has owners and stakeholders from multiple industries that must be included in establishing the performance goals and improving resilience of the components of the system. For resilience of the transmission and distribution communication systems, service provider representatives, including designer professionals (engineers and architects for buildings owned by service providers such as Central Offices/data centers), planners, utility operators, and financial decision makers (i.e., financial analysts) for power service providers must be included in the process. Additionally, representatives of end-users from different industries should be included to establish the performance goals and improve the resilience of the transfer of the communications system from the provider to the building owner. Specifically, transfer of telecommunications and internet to a building is often through a single-point of failure. Hence, those involved in building design, such as planners, architects, engineers, and owners need to be aware of potential opportunities to increase redundancy and resiliency.

Performance goals in this document are defined in terms of how quickly the functionality of the infrastructure can be recovered after a disaster event. Minimizing downtime can be achieved during the design process. An example table of performance goals for communications infrastructure, similar to the format presented in the Oregon Resilience Plan (OSSPAC 2013), is presented in Table 8-1. The performance goals shown in Table 8-1 are not recommendations for which communities should strive to achieve. Rather, the table is intended as a guide that communities/owners can use to evaluate their strengths and weaknesses in terms of the resilience of their communications systems infrastructure. It is recommended that communities and stakeholders use the table as a tool to assess what their performance goals should be based on their local social needs. Tables similar to that of Table 8-1 can be developed for urban and rural communities, any type of disaster event, and for the various levels of hazards (routine, expected and extreme) defined in Chapter 2 of the framework.

Table 8-1 presents an example of suggested performance goals for different components of the communications infrastructure when subjected to an “expected” event. The red shaded boxes indicate the desired time to have 30% functionality of the component. Yellow indicates the time frame in which 60% operability is desired and green indicates greater than 90% operability. We do not set a goal specifically for 100% operability in this example because it may take significantly longer to reach this target and may not be necessary for communities to return to their normal daily lives. The performance of many of the components in the communication network, such as towers and buildings housing equipment are expected to perform according to their design criteria. Recent history; however, suggests that this is frequently not the case.

We have put an “X” in the first two rows of Table 8-1 as an example of how a community can indicate the expected performance and recovery of the infrastructure in their evaluation. As seen in Table 8-1, the “X” indicates that there is a significant gap between what is desired and what reality is for the Central Offices (i.e., buildings that house telephone exchanges) and their equipment. This is a resilience gap. If the community decides that improving the resilience of their Central Offices is a top priority after its evaluation of their infrastructure, the next step would be to determine how to reduce this resilience gap. For Central Offices and their equipment, there are a number of solutions that can help to narrow the gap in resilience, including hardening the building to resist extreme loads and protecting equipment hazards such as flooding by elevating electrical equipment and emergency equipment above extreme flooding levels. These lessons have been learned through past disasters, including the 9-11 terrorist attacks, Hurricane Sandy, Hurricane Katrina, and others.

As previously discussed, the performance goals may vary from community-to-community based upon its needs. It is recommended that representatives of the stakeholders in a given community participate in establishing the performance goals and evaluating the current state of the systems. As discussed throughout the framework, contributions to community resilience include those from design professionals (e.g., engineers and architects), planners, utility operators, regulatory agencies, emergency management planners and first responders, business and political leaders, communications providers, financial analysts, etc. The City of San Francisco provides an excellent example of what bringing together stakeholders can accomplish. San Francisco has developed a lifelines council (The Lifelines Council of the City and County of San Francisco 2014), which brings together different stakeholders to get input regarding the current state of infrastructure and how improvements can be made in practice. The lifelines council performs studies and provides recommendations as to where enhancements in infrastructure resilience and coordination are needed (The Lifelines Council of the City and County of San Francisco 2014). Their work has led to additional redundancy being implemented into the system in the Bay Area.

Table 8-1. Example of Systems Performance Goals for Expected Event to be Developed by Community and/or Stakeholders

System Component	Phase 1 (1-7 Days)			Phase 2 (1-8 Weeks)			Phase 3 (2-36 Months)		
	0-24 hrs.	1-3 days	3-7 days	1-2 wks.	2-4 wks.	1-2 mos.	2-6 mos.	6-12 mos.	1-3 yrs.
Central Office Buildings				X					
Central Office Equipment					X				
Transmission Wires for Critical Facilities (e.g., police, fire, ambulance, hospitals)									
Transmission Wires for residences and businesses									
Overhead Telephone Wires									
Underground Telephone Wires									
Internet Exchange Points									
Internet Backbone									
Cellular Phone Towers									

Key to Table:

Example Goal for 30% Restoration = Red shaded box

Example Goal for 60% Restoration = Yellow shaded box

Example Goal for 90% Restoration = Green shaded box.

Example of expected actual performance = X

Difference between the "X" and shaded box in a row is an example of a resilience gap.

NOTE: This table is an example of a tool of that can be used by communities and their stakeholders to evaluate the expected of their infrastructure for a given event, and identify their performance goals based on local social needs. The performance goals shown are not intended to be recommendations for all communities.

8.3. Communication and Information Infrastructure

As seen from the example performance goals presented in Table 8-1 and the discussion in the previous section, there are a number of critical components in the communication and information system infrastructure. This section discusses some of these infrastructure components and their potential vulnerabilities. Components of a telecommunications system are presented in Figure 8-1.

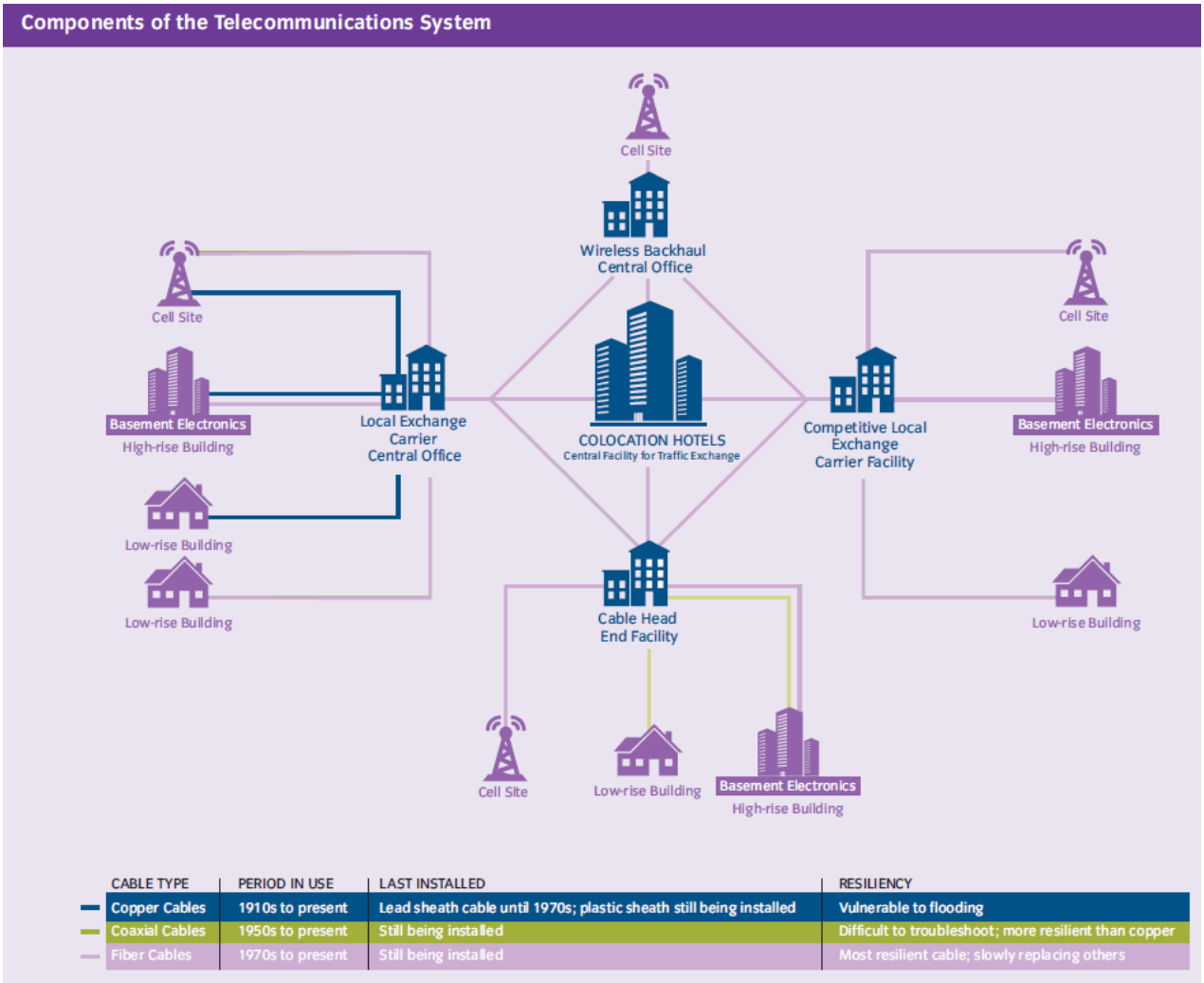

***Figure 8-1. Components of the Communications System* (City of *New York, 2013*)**

8.3.1. Landline Telephone Systems

Most of the newer, high technology communication systems are heavily dependent on the performance of the electric power system. Consequently, these newer communication systems are dependent on the electrical power system, which often is interrupted during and after a disaster, and hence reliable standby power is critical to the continued functionality of the communication network. However, conventional analog landlines (i.e., not digital telephones) operate on a separate electric supply that may not be impacted by the event. Hence, landline telephones are generally, a more resilient option for telephone communication. The American Lifelines Alliance (ALA 2006) recommends that landline systems should be retained or reinstated for standby service to reduce vulnerability.

Central Offices

Central Offices, also known as telephone exchanges, are buildings that house equipment used to direct and process telephone calls and data. Maintaining the functionality of these facilities is critical to the timely recovery from an event. These facilities are designed as occupancy Category III (in some cases IV) buildings in ASCE 7 and consequently would be expected to be fully functional after an expected event.

There are two primary resiliency concerns for Central Offices:

1. Redundancy
2. Design and placement/security of critical equipment

Redundancy of Central Offices

As was learned after the September 11, 2001 (9-11) terrorist attacks on the World Trade Centers in New York City, redundancy of Central Offices is vital to continued service in the wake of a disaster. On September 11th, almost all of Lower Manhattan (i.e., the community most immediately impacted by the disaster) lost the ability to communicate because World Trade Center Building 7 collapsed directly onto Verizon's Central Office at 140 West Street, seen in Figure 8-2 (Lower Manhattan Telecommunications Users' Working Group, 2002). At the time, Verizon did not offer Central Office redundancy as part of its standard service. Furthermore, customers of other carriers that leased Verizon's space lost service as well since they did not provide redundancy either. Verizon made a significant effort to restore their services rapidly after the attacks and have since improved their system to use multiple Central Offices for additional reliability. AT&T also endured similar problems as their entire Central Office was located in World Trade Tower 2, which also collapsed. Overall, almost $2 billion was spent on rebuilding and upgrading Lower Manhattan's telecom infrastructure after 9-11 (Lower Manhattan Telecommunications Users' Working Group, 2002).

Figure 8-2. Damage to Verizon Building on September 11, 2001 (FEMA 2002)

Although this was an extremely expensive venture, it is an example that shows building a telecom system with redundancy can eliminate expensive upgrading/repair costs after a disaster event. Furthermore, this magnitude of expense is likely not necessary for many other communities.

Design of Central Offices and Placement/Security of Critical Equipment

The design of Central Offices is extremely important for continued service of the telecommunications. Depending on the location of the community, the design considers different types and magnitudes of disasters. As previously discussed, these buildings are to be designed as an Occupancy Category III building per ASCE 7, and consequently the design of equipment and standby power must be consistent with that of the building design.

For example, the design of Central Offices in California may be mainly concerned with earthquake loading, whereas Central Offices on the east coast may be concerned mainly with hurricane force winds and/or flooding (especially if it is located in the floodplain as are many Central Offices in coastal communities). In place of providing redundancy of Central Offices, these structures should be designed to resist more extreme environmental loads. In cases where Central Offices are located in older buildings, built to codes and standards which are less stringent than current day standards, it is important to bring these buildings up to modern standards if an acceptable performance level is desired.

Although construction of the building is important; placement and security of equipment is also an essential consideration if functionality is to be maintained. For example, any electrical or standby power equipment, such as generators, should be placed above the extreme (as defined in Chapter 2) flood level scenario, but should also be located such that it is not susceptible to other environmental loads such as wind. The flooding produced by Hurricane Sandy, exposed weaknesses in the location of standby power (e.g., generators). Generators and other electrical equipment that were placed in basements failed due to flooding (FEMA 2013).

In recent events where in-situ standby power systems did not meet the desired level of performance and failed, portable standby power was brought in to help bring facilities back online until the power was restored or the on-site standby generators were restored. For example, Figure 8-3 shows a portable standby generator power unit used in place of basement standby generators that failed due to flooding at a data center in Manhattan, NY after Hurricane Sandy (FEMA 2013).

Since the communities are ultimately responsible for the updating, enforcement and making amendments to building codes, it is important that the most up-to-date building codes are used in the design of buildings used as a part of the communication network.

Figure 8-3. Large Standby Portable Power Unit used when Basement Generators Failed (FEMA 2013)

After 9-11, the Verizon Central Office at 141 West Street (i.e., the one impacted by the collapse of WTC 7) was hardened to prevent loss of service in a disaster event (City of New York, 2013). After 9-11, and prior to Sandy, the 141 West Street Central Office:

- Raised their emergency power generators and switchgear to higher elevations
- Used newer copper infrastructure (i.e., encased the copper wires in plastic casing)
- Provided pumps to protect against flooding

The City of New York compared the performance of this Central Office to one at 104 Broad Street (also affected by Sandy), which had not been hardened. The 104 Broad Street Central Office positioned its emergency power generators and electrical switchgear below grade (i.e., in a basement) and had old copper infrastructure in lead casing (City of New York 2013). While the 141 West Street Central Office (i.e., the hardened Central Office) was operational within 24 hours, the 104 Broad Street Central Office was not operational for 11 days. The success story of the 141 West Street Central Office during and after Sandy illustrates that making simple changes in location of equipment can significantly improve the performance of infrastructure/equipment following a disaster event. It is seen through this example that careful planning of critical equipment location and protection is essential to achieving the performance goal of continued service in the wake of a disaster event.

Placement and security of critical equipment should be considered for all types of natural disasters that a community may experience. As illustrated by the Sandy example, different hazard types warrant different considerations. For earthquake, stability of the equipment must be considered. Figure 8-4 shows an example of failure inside of a Central Office in the 1985 Mexico City Earthquake (OSSPAC 2013). The building itself did not collapse, but light fixtures and equipment failed. Critical equipment in earthquake prone regions should be designed and mounted such that the shaking will not lead to equipment failure.

Figure 8-4. Light Fixture and Equipment Failure inside Central Office in Mexico City 1985 Earthquake (OSSPAC 2013)

As indicated in Chapter 2 and presented in Table 8-1, the desired performance of the communications system in the expected event (as defined in Chapter 2) is little or no interruption of service. These Central Office buildings are considered Risk Category III buildings in ASCE 7 and consequently should be designed to remain functional through the 1/100 year flood elevation + 1 ft, or the design based elevation, whichever is higher, the 1,700 year wind event (based on ASCE 7-10) and the 0.2 percent earthquake. In the case of Hurricane Sandy, the desired performance with respect to flooding was not achieved.

Although these facilities are less vulnerable to wind than flood, in the case of routine, expected and extreme events it is critical that the building envelope performs as intended since failure of the building envelope can allow significant amounts of water to enter the building and damage components. Historically, few building envelopes actually meet the expected performance levels.

Transmission

While the Central Offices of the telecommunications systems play a key role in the functionality of the system, the transmission and distribution system must also be maintained and protected adequately for continued service. There are several components that must be considered for continued functionality.

First/Last Mile Transmission

The “first/last mile” is a term used in the communications industry that refers to the final leg of delivering services, via network cables, from a provider to a customer. The use of the term “last mile” implies the last leg of network cables delivering service to a customer, whereas “first mile” indicates the first leg of cables carrying data from the customer to the world (e.g., calling out or uploading data onto the internet). Although the name implies that it is a mile long, this is not always the case, especially in rural communities where it may be much longer (WV Broadband 2013).

As was learned from the 9-11 attacks, the first/last mile is a key to resilience for telecommunications and information infrastructure, especially for a downtown business’ telecom network. In urban settings, service providers typically connect the Central Offices in a ring, which connects to the internet backbone at several points (Lower Manhattan Telecommunications Users’ Working Group, 2002). The result is a resilient method that improves the likelihood that service providers will achieve their systems

performance goal of continual service because if one node fails in a disaster event, the traffic is redirected to the internet backbone at another point.

In rural communities, there is likely to be less redundancy in the telecommunication and information network cable systems. Historically, rural and remote communities have not used these services as frequently or relied as heavily on them as urban communities. This has been the case because: 1) In the past, the technology to send large amounts of data over a long distance had not been available; and 2) The cost for Service Providers to expand into remote communities may be too high and have a low benefit-cost ratio. As a result of the lack of redundancy in rural and remote communities, a failure of one node in the service cables may be all that is necessary for an outage to occur. Therefore, rural and remote communities may not have the same performance goals as urban communities.

Copper Wires

Copper wires work by transmitting signals through electric pulses and carry the low power needed to operate a traditional landline telephone. The telephone company (i.e., service provider) that owns the wire provides the power rather than an electric company. Therefore, the use of traditional landlines that use copper wire lessens the interdependency on external power (ALA 2006). As a result, in a natural disaster event resulting in loss of external power, communication may still be possible through the use of landlines.

Although copper wires perform well in many cases, they are being replaced more and more by fiber optic cables because copper wires cannot support the large amount of data required for television and high-speed internet, which has become the norm in the 21st century (Lower Manhattan Telecommunications Users' Working Group 2002).

Some service providers are interested in retiring their copper wires. Keeping both fiber optic and copper wires in service makes maintenance expensive for service providers and, hence, for customers (FTTH Council 2013). Copper wire is an aging infrastructure that becomes increasingly expensive to maintain. Verizon has reported that its operating expenses have been reduced by approximately 70% when it installed its FiOS (fiber optic) network and retired its copper plant in Central Offices (FTTH Council 2013).

Despite the advantages of traditional copper wire, there are also well-documented problems. As was seen during and after Hurricane Sandy, copper wire is susceptible to salt water flooding. Once these metal wires are exposed to salt water, they fail (City of New York 2013). One solution to this problem is to ensure that the copper wire is encased in a plastic or another non-water sensitive material. Furthermore, copper wires are older and generally, are no longer being installed.

Coaxial Cables

Coaxial cable is a more modern material and commonly used for transmission. It offers more resistance to water and, therefore, is not as susceptible to damage as are copper wires to flood waters. It was found after Sandy that these wires generally performed well with failures typically associated with loss of power to the electrical equipment to which they were connected (City of New York 2013). Coaxial cable has been and continues to be primarily used for cable television and internet services. However, coaxial cables are being replaced more and more by fiber optic cable since are able to carry all type of services.

Fiber Optic Cables

Fiber optic cables are more resistant to water damage than either coaxial cable or copper wire (City of New York 2013). Fiber optic cables are now commonly used to bundle home services (television, high-speed internet, and telephone) into one system, and to provide ultra-high speed internet. The use of fiber optic cables allows for transmission of large amounts of data on a single fiber. These cables are fully water resistant (City of New York 2013). Unfortunately, these services rely more heavily on power provided by a power company instead of the communications provider itself. Consequently, during and after a natural disaster event where power is frequently interrupted, landline communications using fiber optic cables is lost (ALA 2006). In fact, some communities turn off the power prior to the arrival of hurricane force winds for safety purposes. This prevents "live" electric lines from falling on roads, homes, etc., but it also eliminates the external power source for telecommunications. Some service providers provide in-home battery backup for cable and telephone.

Overhead vs. Underground Wires

Transmission wire can be strung overhead using utility poles or run underground. There are advantages and disadvantages for both options.

Overhead wire failures are relatively easily located and repaired in the wake of a natural disaster. However, their exposure makes them especially susceptible to high wind (e.g. hurricanes and tornadoes) and ice hazards. In high wind events, overhead wires may fail due to the failure of poles by the direct action of wind acting on the poles and cables or trees falling onto the cables. Figure 8-5 shows an example of a failure a (Cable Television) CATV line due to the direct action of wind during Hurricane Katrina.

Figure 8-5. Failure of CATV cable due to the direct action of wind.

Widespread failure of the above-ground system in high winds and ice storms is common and often associated with the effects of tree blow-down and falling branches, and it is difficult to mitigate without removing trees. Some improvement in performance can be achieved with continued trimming of branches, both to reduce the likelihood of branches falling on lines and to reduce the wind-induced forces acting upon the tree which reduces the blow-down probability. Tree trimming is performed by the electric utility which owns the poles. The challenges associated with tree removal and trimming is discussed in Chapter 7.

Ice storms can also result in failure of above ground communication infrastructure. For example, in January 2009, Kentucky experienced an ice storm in which long-distance telephone lines failed due to icing on poles, lines and towers, and loss of power (Kentucky Public Service Commission 2009). Similarly to wind hazards, the accumulation of ice seen in Kentucky, paired with snow and high winds led to tree fall onto overhead telephone and power lines. However, unlike power lines, telecommunication lines that have limbs hanging on them or fall to the ground will continue to function unless severed (Kentucky Public Service Commission 2009). Since long-distance telecommunications are dependent on power from another source (i.e., power providers), communication with those outside of the local community were lost during the storm. As was seen following the 2009 Kentucky ice storm, many communities became isolated and were unable to communicate their situation and emergency needs to regional or state disaster response officials (Kentucky Public Service Commission 2009).

Emergency response and restoration of the telecommunications infrastructure after a disaster event is an important consideration for which the challenges vary by hazard. In the case of both high wind and ice/snow events, tree fall on roads (Figure 8-6) slows-down emergency repair crews from restoring power and overhead telecommunications. Ice storms have their own unique challenges in the recovery process. In addition to debris (e.g., trees) on roads, emergency restoration crews can be slowed down by ice-covered roads, and soft terrain (e.g., mud) in rural areas. Emergency restoration crews also face the difficulties of working for long periods of time in very cold and windy conditions which can be associated with these events. Therefore, communities must consider the conditions under which emergency restoration crews must work in establishing realistic performance goals of telecommunications infrastructure.

Figure 8-6. Trees Fallen across Roads due to Ice Storm in Kentucky Slowed Down Recovery Efforts (Kentucky Public Service Commission 2009)

Although installation of underground wires eliminates the concern of impacts from wind and tree fall, it is much more expensive to install and maintain the wires. Furthermore, if there is a failure, it is much more difficult to locate and repair. Underground wires may also be more susceptible to flood if not properly protected, or earthquake damage and liquefaction.

8.3.2. Internet Systems

The internet has become the most used source of one and two-way communication over the past couple of decades. It is continually used for email, online shopping, receiving/reading the news, telephony, and increasingly for use of social-networking. Businesses have become heavily reliant on the internet for such things as communication, sending and receiving documents, performing video conferencing, email, and working with other team members using online collaboration tools. The internet is heavily used by financial institutions for transferring funds, buying and selling stocks, etc. As healthcare moves towards electronic medical records, connectivity is becoming more and more important in the healthcare system.

High-speed internet is often tied in with telephone and cable by service providers through the use of coaxial or fiber optic wires. The internet is dependent on the electric power system and loss of power at any point along the chain from source to user prevents data reception. As a result, the internet's dependency on the electric power system makes it vulnerable to the performance of the power system in a natural disaster event. A concern for internet systems, as is the case for landlines, is single points of failure (i.e., an individual source of service where there is no alternative/redundancy).

Internet Exchange Points (IXP)

Internet Exchange Points are buildings that allow service providers to connect directly to each other. This is advantageous because it helps improve quality of service and reduce transmission costs. The development of IXPs has played a major role in advancing the development of the internet ecosystem across North America, Europe, and Asia (Kende and Hurpy, 2012). IXPs are now also stretching into several countries in Africa and continue expand the reach of the Internet. IXPs facilitate local, regional, and international connectivity.

IXPs provide a way for its members, including Internet Service Providers (ISPs), backbone providers and content providers to connect their networks and exchange traffic directly (Kende and Hurpy 2012). Similarly to Central Offices for landlines, this results in IXPs being a potential single point of failure.

The building housing the IXP's would be expected to meet the ASCE 7 requirements for critical buildings (Occupancy Category IV) and consequently would be expected to perform with no interruption of service for the "expected" event, or hazard level. The facilities would be expected to have sufficient standby power to function until external power to the facility is brought back online.

Location of Critical Equipment in IXPs

Another similarity to Central Offices of the telecommunications system is that the location and protection of critical equipment is important. Critical equipment should be protected by placing it in locations where it will not be susceptible to the expected hazards in the community. For example, it is inevitable that some of these buildings will be or have been built in floodplains because many large urban centers are centered around large bodies of water or on the coast.

The owner, engineers, maintenance, and technical staff must all be aware of the potential hazards that could impact the equipment within the structure. As should be done for Telecommunications Central Offices, the following considerations should be taken into consideration for the critical equipment of IXPs:

- Electrical and emergency equipment should be located above the elevation of an "extreme" flood, which is to be defined by the community.

- Rooms housing critical equipment should be designed to resist the extreme loads for the community, whether it is earthquake, high wind, blast, other hazards, or a combination of hazards. Remember that fire is often a secondary hazard that results from other disaster events.
- Where possible, redundancy and standby power for critical equipment should be provided.

All too often in the past, communities have seen the same problems and damage in the wake of a natural disaster event (e.g., loss of power, loss of roof cover and wall cladding leading to rain infiltration in high wind events). Fortunately, many of the problems can be mitigated by sufficient planning and assessment of the risks. As previously discussed, a great example of this was the comparison of two Telecommunications Central Offices in New York City after Hurricane Sandy. Careful placement and protection of critical equipment can help to achieve the performance goals of the internet's critical equipment. For example, in flood prone regions, critical equipment should be placed above the extreme flood level for the area. In earthquake regions, critical equipment should be designed and mounted such that shaking from earthquake events does not cause failure.

Internet Backbone

The Internet Backbone refers to the cables that connect the "network-of-networks." The Internet is a system of nodes that are connected by paths/links. These paths run all over the United States and the rest of the world. As a result, many of the same challenges identified for the landline cables for fiber optic cables exist for internet, namely that it requires power to function. Therefore, the heavy reliance on power impacts the performance and recovery goals of internet service for service providers and their customers.

Path Diversity

Path diversity refers to the ability of information to travel along different paths to get to its destination should there be a failure in its originally intended path (i.e., path diversity is synonym of redundancy). The more diversity that exists, the more reliable the system will be.

8.3.3. Cellular/Mobile Systems

The cellular telephone system has most of the same possible points of failure as the landline system, including the local exchange offices, collocation hotels, and cable head facilities. Other possible failure points unique to the cellular network include the cell site (tower and power) and wireless backhaul Central Offices. Figure 8-1 shows how the cellular phone network fits within the telecommunication network. At the base of a cell tower is switchgear and standby power. Damage to the switchgear at the base of the tower prevents the transmission of data thorough to local exchanges, etc.

8.3.3.1. Cell Towers

Virtually all natural hazards including earthquake, high wind, ice and flood affect the ability of an individual cell tower to function through one or more of the following.

Loss of external power.

Large scale loss of external power occurs relatively frequently in hurricanes (mainly due to high wind and flooding), large thunderstorm events (such as those associated with derechos and tornadoes), ice storms, and earthquakes. Most cell towers are equipped with batteries that are designed to provide 4 to 8 hours of standby power after loss of external power (City of New York 2013). Figure 8-7 shows an example of a cell tower with standby power and switchgear at the base. The functionality of the tower can be extended through the use of permanent or portable diesel generators. Portable generators were used in the New York following Hurricane Sandy in 2012. The installation of permanent diesel generators has been resisted by the providers due to the high cost and practicality (City of New York 2013).

Recalling that buildings and systems should remain fully functional during and after a routine event (Chapter 2), all cellular towers and attached equipment should remain operational. There is an expectation that the 9-1-1 emergency call system will remain functional during and after the event. Considering the poor performance of the electric grid experienced during recent hurricanes (which produced wind speeds less than the nominal 50 to 100 year values as specified in ASCE 7 [93, 95, 02 and 05]), external power is unlikely to remain functional during the expected, or even routine (as defined in Chapter 2) event. Consequently, adequate standby power is critical to ensure functionality. Recent experience with hurricanes and other disaster events suggest that the standby power needs to last longer than the typical current practice of four to eight hours (City of New York 2013).

Figure 8-7. Base of Cell Tower Showing Standby Power and Switch Gear

In flood prone areas the standby power needs to located, at a minimum, above the 100 year flood level to ensure functionality after the event. Similarly, the equipment must be resistant to the 50 year earthquake load.

The use of permanently located diesel electric standby power poses significant difficulties due to the initial and ongoing required maintenance costs. Diesel generators are loud and will invariably generate significant complaints from nearby residents. In the case of events, such as hurricanes and major ice storms, where advanced warning is available, portable generators can be staged and deployed after the storm. The portable generators usually require refueling about once per day so continued access is

important. In events where there is little to no warning, such as earthquakes and tornadoes, staging of portable generators cannot be completed ahead of time.

In highly urbanized areas, such as New York City, cell towers are frequently located on top of buildings, preventing the placement of permanent diesel standby generators and making it difficult to supply power from portable generators because of impeded access.

Improvements in battery technology and the use of hydrogen fuel cell technologies may alleviate some of the standby power issues. Furthermore, newer cellular phone technologies require less power, potentially leading to longer battery life. Standby battery technology is a key consideration in establishing the performance goals of cellular phones in the wake of a disaster event.

Failure of Cell Phone Towers.

Collapse of cell phone towers due to earthquake, high winds, or flooding should not be expected to occur when subject to a natural disaster event of magnitude less than or equal to the expected event. This was not the case in Hurricane Katrina (2005) where cell phone towers were reported to have failed (DHS, 2006), although many failed after being impacted by flood-borne debris (large boats, etc.), whose momentum was likely well beyond a typical design flood impact. Figure 8-8 shows an example of a cell phone tower that failed due to high winds in Hurricane Katrina. After an event, failed towers can be replaced by temporary portable towers. Similarly, the January 2009 Kentucky ice storm had cell phone tower failures due to the combination of ice accumulation and winds over 40 mph (Kentucky Public Service Commission 2009).

Cell towers are designed to either ASCE Category II or ASCE Category III occupancy requirements. The latter is used when the towers are used to support essential emergency equipment or is located at a central emergency hub. Consequently, in the case of wind and flood, the towers and equipment located at the base of the tower should perform without any damage during both the routine and expected events (Chapter 2).

Figure 8-8. Tower Failed Due to Wind During Hurricane Katrina.

8.3.3.2. Backhaul facilities

Backhaul facilities serve a purpose similar to that of the Central Offices and consequently should meet the same performance goals, including proper design of the standby power system.

8.4. Regulatory Environment

There are multiple regulatory bodies at the various levels of government (Federal, State, and Local) that have authority over communications infrastructure. There is no one regulatory body that oversees all communication infrastructure and is responsible for enforcement of the various standards and codes. Furthermore, the rapidly evolving technologies over the past 30 years have led to changes in regulatory jurisdiction, which adds complexity to the regulatory environment. This section discusses regulatory bodies of communications infrastructure at the Federal, State, and Local levels.

8.4.1. Federal

The regulatory body of communication infrastructure is the FCC. The FCC is a government agency that regulates interstate and international communications of telephone, cable, radio and other forms of communication. Therefore, it has jurisdiction over wireless, long-distance telephone, and the Internet (including VoIP).

As discussed earlier in this chapter, the FCC has a Communications Security, Reliability, and Interoperability Council (CSRIC) that promotes best practices. The council performs studies, including after disaster events, such as Hurricane Katrina, and recommends ways to improve disaster preparedness,

network reliability, and communications among first responders Victory et. al (2006). However, the recommended best practices are not required to be adopted and enforced.

8.4.2. State

State government agencies have authority over local landline telephone service. Most commonly, the agency responsible for overseeing communications infrastructure at the State level is known as the Public Service Commission (PSC). However, other State agencies have jurisdiction over telecommunications infrastructure as well. A prime example is the State DOT. The State DOT has jurisdiction over the right-of-way and, therefore, oversees construction of roads/highways where utility poles and wires are built. Utility poles and wires are commonly placed within the right-of-way of roads, whether it is above ground or underground. The DOT has the ability to permit or deny planned paths of the utilities.

8.4.3. Local

Local government has jurisdiction over communication infrastructure through a number of agencies. The Department of Buildings (DOB), or equivalent, is responsible for enforcing the local Building Code. Therefore, the DOB regulates the placement of electrical equipment, standby power, and fuel storage at critical telecommunications facilities such as Central Offices (City of New York 2013).

Large cities, such as New York City, Chicago, Los Angeles, and Seattle have their own DOT (City of New York 2013). These local DOTs oversee road construction and the associated right-of-way for utilities (including communications infrastructure). Many smaller municipalities have an Office of Transportation Planning, which serves a similar function.

8.4.4. Overlapping Jurisdiction

Due to the complex bundling packages that service providers now offer customers, there are a number of regulatory bodies that have jurisdiction over the various services provided in said bundle. For example, a bundled telephone, Internet and cable package by both Local (cable) and Federal (Internet and VoIP) agencies (City of New York 2013). Furthermore, changing from traditional landlines to VoIP shifts a customer's services from being regulated by State agencies to Federal agencies. As technology continues to evolve, jurisdiction over services may continue to shift from one level of government to another. Following the current trend of more and more services becoming Internet based, the shift of services may continue to move toward being under Federal agency regulations.

8.5. Standards and Codes

Codes and Standards are used by the communication and information industry to establish the minimum acceptable criteria for design and construction. The codes and standards, shown in Table 8-2, were mainly developed by the American National Standards Institute/Telecommunications Industry Association (ANSI/TIA). This organization has developed many standards that are adopted at the state and local government levels as well as by individual organizations. In fact, many of the standards presented in Table 8-2 are referenced and adopted by universities, such as East Tennessee State University (ETSU 2014), in their communication and information systems design guidelines. Individual end-users, such as a university campus or hospital, and levels of government may have additional standards/guidelines.

Table 8-2. Summary of Communication and Information Codes and Standards

Code/Standard	Description
ANSI/TIA-222-G Structural Standards for Antennae Supporting Structures and Antennas	Specifies the loading and strength requirements for antennas and their supporting structures (e.g., towers). The 2005 edition of the standard has significant changes from its previous editions including: changing from ASD to LRFD; change of wind loading to better match ASCE-7 (i.e., switch from use of fastest-mile to 3-second gust wind speeds); updating of ice provisions; and addition of seismic provisions (Erichsen 2014).
ANSI/TIA-568-C.0 Generic Telecommunications Cabling for Customer Premises	Used for planning and installation of a structured cabling system for all types of customer premises. This standard provides requirements in addition to those for specific types of premises (Anexter Inc. 2013).
ANSI/TIA-568-C.1 Commercial Building Telecommunications Cabling Standard	Used for planning and installation of a structured cabling system of commercial buildings (Anexter Inc. 2013).
ANSI/TIA-569-C Commercial Building Standard for Telecommunication Pathways and Spaces	Standard recognizes that buildings have a long life cycle and must be designed to support the changing telecommunications systems and media. Standardized pathways, space design and construction practices to support telecommunications media and equipment inside buildings (Anexter Inc. 2013).
ANSI/TIA-570-B Residential Telecommunications Cabling Standard	Standard specifies cabling infrastructure for distribution of telecommunications services in single or multi-tenant dwellings. Cabling for audio, security, and home are included in this standard (Hubbell Premise Wiring, Inc. 2014)
ANSI/TIA-606-B Administration Standard for Commercial Telecommunications Infrastructure	Provides guidelines for proper labeling and administration of telecommunications infrastructure (Anexter Inc. 2013).
ANSI/TIA-942-A Telecommunications Infrastructure Standard for Data Centers	Provides requirements specific to data centers. Data centers may be an entire building or a portion of a building (Hubbell Premise Wiring, Inc. 2014).
ANSI/TIA-1005 Telecommunications Infrastructure for Industrial Premises	Provides the minimum requirements and guidance for cabling infrastructure inside of and between industrial buildings (Anexter Inc. 2013).
ANSI/TIA-1019 Standard for Installation, Alteration & Maintenance of Antenna Supporting Structures and Antennas	Provides requirements for loading of structures under construction related to antenna supporting structures and the antennas themselves (Anexter Inc. 2013).

Table 8-2. Summary of Communication and Information Codes and Standards (Continues)

Code/Standard	Description
ANSI/TIA-1179 Healthcare Facility Telecommunications Infrastructure Standard	Provides minimum requirements and guidance for planning and installation of a structured cabling system for healthcare facilities and buildings. This standard also provides performance and technical criteria for different cabling system configurations (Anexter Inc. 2013).
ASCE 7-10 Minimum Design Loads for Buildings and Other Structures	Provides minimum loading criteria for buildings housing critical communications equipment. Also provides loading criteria for towers.
IEEE National Electrical Safety Code (NESC)	United States Standard providing requirements for safe installation, operation and maintenance of electrical power, standby power and telecommunication systems (both overhead and underground wiring).

8.5.1. New Construction

This section is under development. Text to be included in a future draft.

8.5.1.1. Performance Levels

This section is under development. Text to be included in a future draft.

8.5.1.2. Hazard Levels

This section is under development. Text to be included in a future draft.

8.5.1.3. Recovery Levels

This section is under development. Text to be included in a future draft.

8.5.2. Existing Construction

This section is under development. Text to be included in a future draft.

8.5.2.1. Performance Levels

This section is under development. Text to be included in a future draft.

8.5.2.2. Hazard Levels

This section is under development. Text to be included in a future draft.

8.5.2.3. Recovery Levels

This section is under development. Text to be included in a future draft.

8.6. Reliability v. Resilience

This section is under development. Text to be included in a future draft.

8.7. Resilience Needs

As with all design codes and standards, those applicable to communication and information infrastructure provide minimum requirements. However, to develop resilient infrastructure, vulnerabilities in the codes and standards must be identified and improvements recommended to narrow the resilience gaps. Furthermore, research in some areas is needed to develop new, innovative solutions to vulnerabilities that exist in current standards.

8.7.1. Standards and Codes

The codes and standards identified in Section 8.5 are presented again in Table 8-3. The table identifies areas of the codes and standards that are recommended to be improved upon.

Table 8-3. Communication and Information Sector Codes and Standards

Codes/Standards	Vulnerabilities	Improvements
ANSI/TIA-222-G Structural Standards for Antennae Supporting Structures and Antennas		*This table is under development. To be completed for a future draft.*
ANSI/TIA-568-C.0 Generic Telecommunications Cabling for Customer Premises		
ANSI/TIA-568-C.1 Commercial Building Telecommunications Cabling Standard		
ANSI/TIA-569-C Commercial Building Standard for Telecommunication Pathways and Spaces		
ANSI/TIA-570-B Residential Telecommunications Cabling Standard		
ANSI/TIA-606-B Administration Standard for Commercial Telecommunications Infrastructure		
ANSI/TIA-942-A Telecommunications Infrastructure Standard for Data Centers		
ANSI/TIA-1005 Telecommunications Infrastructure for Industrial Premises		
ANSI/TIA-1019 Standard for Installation, Alteration & Maintenance of Antenna Supporting Structures and Antennas		
ANSI/TIA-1179 Healthcare Facility Telecommunications Infrastructure Standard		
ASCE 7-10 Minimum Design Loads for Buildings and Other Structures		
IEEE National Electrical Safety Code (NESC)		

8.7.2. Practice and Research Needs

This section is under development. Text to be included in a future draft.

8.8. Summary and Recommendations

The telecommunications system has changed dramatically over the past 20-30 years. Constant communication has become an essential part of people's daily lives and becomes even more important in the immediate wake of a disaster.

- Emergency Response personnel need to communicate with one another and those who are injured, trapped, etc.
- Individuals need to communicate with their loved ones and check on each other's safety.
- Low-income, elderly, and disabled or special needs populations are primary concerns during and after a disaster event.
- Businesses and organizations need to re-establish themselves quickly and re-connect with their customers and suppliers.
- Local government needs to continue governance, provide updates to the community, and coordinate with outside help via the state and/or federal government.
- Restoration of the communication.

Two main points are evident in this chapter with respect to the resilience of communications infrastructure:

1. Building redundancy into telecommunications infrastructure is a key.
2. Ensuring buildings housing key components of the communication system are designed to, or brought up to current day standards, including the location of standby power, switchgear etc. is critical if these important parts of the communication network are to perform as desired during and after a natural hazards event. Adoption, administration and enforcement of the latest national standards and building codes at the community level are critical to ensure properly designed and built facilities.

The following are recommended for consideration by communities:

- Bring together a group of the stakeholders to form a Communication Infrastructure Council
    - The first step to get buy-in from the key entities, such as the service providers, building officials, local government is to get them involved in the process early and often. If stakeholders work together so that the entire community benefits, including themselves, the council is much more likely to succeed.
- An assessment of the current state of the Communications Infrastructure and its' vulnerabilities within the community should be completed
    - This activity can be carried out by the Communication Infrastructure Council
    - The example table of recommended performance goals in this Chapter can be used as a tool to identify the gaps between the actual and desired levels of resilience of a component of the system. The community can then use their findings to prioritize their needs and develop an action plan to make improvements over time with available funding.

  - The community can also adjust the recommended performance goals to fit the needs of that individual community.

- Look for opportunities to add redundancy to existing systems.
  - Funding is always an issue and so there is no expectation that everything will change at once. However, communities and service providers should work to look for opportunities to add redundancy to components of their infrastructure whenever possible. Redundant systems allow for a better chance of continued service in the event of a failure of a part of the system.

- Buildings and structures are designed to minimum criteria to resist hazards based on the applicable codes and standards (e.g., ASCE 7). If the structure being designed is known to be a single point of failure, the owner should consider having the structure hardened or designed to a higher standard. In Chapter 2 of this Framework, we provide definitions for different magnitudes of hazard. The nominal design criteria presented in correspond to the "expected" event but load and resistance factors (or safety factors) have been applied so it is expected that structures built to these standards will survive without damage sufficient to cause service interruption during the extreme event. However, for single points of failure, it is suggested that the design criteria should be consistent with the "extreme" event (ASCE Occupancy Category IV).

  The design and placement of key electrical components, standby power, etc. needs to be consistent with the overall performance goals of the building as a whole. In the case of flooding, for example, meeting the ASCE 7 design criteria and providing a risk consistent structural design requires placing critical equipment, electric panels, emergency equipment etc., at the appropriate height above the BFE or flood proofing the structure to prevent water intrusion during the extreme event.

8.9. References

Anixter Inc., (2013). *Standards Reference Guide.* Glenview, Illinois.

American Lifelines Alliance (2006). *Power Systems, Water, Transportation and Communications Lifeline Interdependencies – Draft Report.* Washington, DC.

American Society of Civil Engineers (ASCE 2010). *ASCE 7-10, Minimum Design Loads for Buildings and Other Structures, Second Edition.* New York, New York.

The City of New York (2013). *A Stronger, More Resilient New York.* New York City, NY.

East Tennessee State University Office of Information Technology (ETSU 2014). *Telecommunications Design and Installation Standards Policy.*

Erichsen, John R. *Slideshow Presentation: ANSI/TIA-222-G Explained.* Viewed July 5, 2014.

Fiber-to-the-Home Council (FTTH Council 2013). *Comments of the Fiber-to-the Home Council on Request to Refresh Record and Amend the Commission's Copper Retirement Rules.* Washington, DC.

Hubbell Premise Wiring Inc. *Structured Cabling Standards and Practices.* Viewed July 5, 2014.

Kende, Michael, and Hurpy, Charles (2012). *Assessment of the Impact of Internet Exchange Points – Empirical Study of Kenya and Nigeria.* Analysys Mason Limited. Washington, DC.

Kentucky Public Service Commission (2009). *The Kentucky Public Service Commission Report on the September 2008 Wind Storm and the January 2009 Ice Storm.*

Lower Manhattan Telecommunications Users' Working Group Findings and Recommendations (2002). *Building a 21st Century Telecom Infrastructure.* Ney York City, NY.

Oregon Seismic Safety Policy Advisory Commission (OSSPAC 2013). *The Oregon Resilience Plan: Reducing Risk and Improving Recovery for the Next Cascadia Earthquake and Tsunami.* Salem, Oregon.

The Lifelines Council of the City and County of San Francisco (2014). *Lifelines Interdependency Study Report I.* San Francisco, California.

Federal Communications Commission (FCC 2011). <www.fcc.gov/telecom.html>. Viewed on July 5, 2014. *Telecommunications Act of 1996.*

Federal Emergency Management Agency (FEMA 2013). *Mitigation Assessment Team Report: Hurricane Sandy in New Jersey and New York.* Washington, DC.

West Virginia Broadband (2013). Viewed July 5, 2014. <http://www.westvirginia.com/broadband/mediaroom/BroadbandGlossary.pdf>.

Victory, Nancy et al. (2006). *Report and Recommendations of the Interdependent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks.* Washington, DC.