The Verizon Wireless Business Continuity and Disaster Recovery program is just one part of our overall philosophy to provide high quality services for our customers. Our nationwide wireless network is at the core of our business, and we have invested more than $111 billion since the company was formed – averaging over $6 billion every year – to increase coverage and capacity and to add new services.

Our Business Continuity and Disaster Recovery ("BC/DR") program team is responsible for minimizing the impact of a disruption to our customers, employees, infrastructure, and business operations. We accomplish this objective by focusing on the following activities:

- Identify critical functions, infrastructure and risks;
- Implement strategies to minimize the risk of a disruption;
- Develop Business Continuity and Disaster Recovery plans, and Crisis Management Teams to recover operations in the event of a disruption;
- Maintain BC/DR plans, with updates completed at least annually;
- Test our plans, at least annually, to validate our response capabilities.

We continue to refine our response and recovery capabilities due to the increasing variety of services we provide and the ever-changing level of potential threats to these services.

The cross-functional Crisis Management Teams in place across our national footprint enhance coordination and response activities during crisis events. These teams provide a command-and-control structure that allows management to gather and report information about crisis events, for the teams to escalate decision-making as needed, and to facilitate resource allocation.

BC/DR activities are visible across all major aspects of our company. We have developed numerous plans to recover critical functions. Business functions have implemented strategies and procedures that not only support routine operations, but also help the function continue to operate in the event of a disaster. Robust operational strategies are at the core of our ability to provide reliable and resilient services.

This document provides additional information regarding pro-active planning activities in three of our major customer-affecting departments: Network Operations, Information Technology and Customer Service.
Network Operations – Our wireless network is resilient by design

The Verizon Wireless network operations philosophy is driven by the desire to provide our customers with an extremely high level of service.

Verizon Wireless strives to deliver superior service based on our design philosophy, which includes redundancy on critical paths and components so that a potential failure of a network component does not significantly affect our customers. Our wireless services are provided through a large and sophisticated national network of 137 Mobile Switching Centers (“MSCs”) and Data Centers throughout our service areas. We will continue to invest in our network to support our customers.

The wireless voice and data switching networks are designed to provide continuous service to the customer. The communications between our internal switches and external networks such as the Public Switched Telephone Network (“PSTN”) and the Internet are also designed to reduce the possibility of interrupted communications. The use of battery and generator backup systems in critical locations also serves to minimize the risk of a disruption, if commercial power is lost.

Our design concept extends from our equipment and technology capabilities to our business procedures. These procedures include frequent and thorough preventive maintenance, real-time monitoring of all key system components, the 24x7x365 availability of trained maintenance personnel to repair or resolve critical failures should they arise, and wide deployment of these personnel and spare parts to permit rapid response and restoration of service.

Our most critical recovery assets are the thousands of highly-trained and experienced network technicians who have repeatedly proven their ability to respond, troubleshoot problems, and restore service to our customers during emergency situations.

Monitoring, maintenance, and restoration of wireless services

Service protection and restoration strategies are an integral part of Verizon Wireless network management and operations.

We have two Network Operations Centers (“NOCs”), one located in New Jersey and another in Texas, that monitor all facilities, cell sites and switches across our nationwide network. These NOCs are staffed 24x7x365 with experienced personnel who work closely with our regional field operations teams and with our vendors to coordinate and expedite the restoration of service in the event of outages. Each NOC receives alarms or other indicators that help troubleshoot problems in the network, and that provide technicians with key information to analyze and maintain network integrity.

The NOC technicians work with the field operation managers, and personnel are dispatched to the affected site as needed. An inventory of standard spare parts and repair equipment is available to technicians in all of our central network locations. We also have standing agreements with our critical vendors to get 24x7 support from their engineering personnel and obtain replacement equipment if required.
Strategy for continued service to Mobile Switching Centers ("MSCs")

Mobile Switching Centers are an important part of our national wireless network, and we continue to add them to our network as we grow. We have 139 MSCs strategically distributed across the country to meet the needs of our customers. Our teams monitor the loading of the switching and data systems to maintain an optimum capacity and service level. One goal of this is to reduce the impact of a disaster to any one MSC. Available capacity in neighboring MSCs could be utilized in the event of a serious disaster.

In addition to redundancy in the equipment and circuitry, each MSC is protected by automatic power backup systems, by automatic fire detection and suppression systems, and by physical security systems and alarms. MSC buildings have restricted access to prevent entry by unauthorized personnel. The building structure itself is designed to provide protection for the systems and services located inside.

In each MSC, network operations personnel routinely backup system data for the switch itself and the peripheral systems. Automated backup routines are supplemented with scheduled manual backup routines and off-site storage of critical data.

A disaster recovery plan has been developed for each MSC, which addresses the recovery of the systems, services and personnel. These plans are updated at least annually. Exercises are conducted at least annually to confirm that these plans can be implemented as expected and to continually increase the readiness of the network teams to respond to an actual disaster. These exercises focus on disasters that may impact us or our customers.

Strategy for continued service to cell sites

We have thousands of cell sites across our nationwide network to provide the desired level of customer service, both in terms of capacity and quality of service. Despite the large number of sites, the loss of a single cell site is still a serious situation. We take extra precautions to protect and keep cell sites operational.

Cell site operations are protected in many ways, including redundancy in the equipment, automatic power backup systems, automatic fire detection systems, and by physical security systems and alarms. Through arrangements with our vendors, any major components of a cell site, up to and including the building and tower, becomes an immediate priority restoration effort on the part of both Verizon Wireless and our vendors.

Cell site equipment has sophisticated diagnostics that can instantly determine if a problem occurs at the site. These diagnostic alarms are transmitted to the MSC, which is monitored by regional field operations teams, and the NOC. Cell sites are outfitted with backup batteries, and in most cases backup generators in case of commercial power loss.

We maintain and utilize portable cell sites referred to as Cells-on-Wheels ("COWs") and Cell-on-Light-Trucks ("COLTs"), which are fully functional generator-powered cell sites that can replace or enhance network coverage and capacity in a given area. They can accommodate both voice and data services, and can be used for emergency situations. For example, they can be used to enhance communications between firefighters when they are fighting a fire in a remote wilderness area. These portable cell sites are
strategically located throughout our network coverage areas and may be deployed to an area that is affected by a weather-related or other disaster.

**Backup power strategy for the wireless network**

Verizon Wireless purchases power from electric companies for the day-to-day power requirements of our network infrastructure. If commercial power is lost, we have implemented backup power systems for all of the critical equipment and infrastructure in our wireless network.

This is accomplished by installing large banks of backup batteries in our MSCs and Data Centers, and these are supported by permanent backup generators. We have arrangements with our fuel suppliers to refill our fuel tanks as needed, allowing our systems to operate until commercial power is restored.

The cell sites are also equipped with batteries, and most sites also have permanent generators which turn-on automatically if commercial power is lost. The company also owns a large supply of portable generators that can be deployed to provide emergency power during extended power outages to those cell sites without permanent generators.

Our MSC, Data Center, and cell site generators are tested regularly to ensure that they are functioning properly. Both the batteries and generators are regularly put through rigorous load tests to ensure that they can support the needs of the network in the event of a commercial power disruption.

**Circuit diversity strategy for the wireless network**

Our wireless network is comprised of numerous components that are connected using a mixture of fiber optic and high bandwidth telecommunication circuits. We support many of our critical network locations with diverse circuits, network technologies, and alternate local telecom carriers. The impact of a severed fiber optic cable or a faulty data circuit is minimized by this diversity in our telecommunications connectivity.
Information Technology – Disaster Recovery Planning

The Information Technology ("IT") team for Verizon Wireless manages the technology that supports internal business functions. For example this technology helps internal users respond to customer needs, streamline internal and external communications, and automate many of our high volume activities. Many of these technologies are integral to our daily operations.

Our IT Disaster Recovery team focuses its efforts on mission critical applications and systems, many of which support customer transactions. System engineers for these applications and their supporting technologies emphasize redundancy, geographic diversity, and heightened security to safeguard these systems from an unexpected interruption or disaster.

Data Center Strategy

Mission critical applications are maintained in a secure data center environment. Our major data centers are protected by automatic fire detection and suppression systems, and by physical security systems and alarms. The data centers have strictly limited access to prevent entry by unauthorized personnel. Only a small number of authorized employees are permitted to access these data centers, and the buildings are monitored by security guards and camera systems to provide a high level of protection to the systems and services located there.

All data centers are backed up by both battery and permanent generator systems which are designed to support the data center for extended timeframes in the event commercial power is disrupted. These systems are tested regularly to ensure that they will provide power when needed.

Data Backup Strategy

In each of the Data Centers that house mission critical applications, a significant amount of resources are put into our data back-up and restoration capabilities. Ensuring the availability and security of critical historic data is part of daily operations, and our back-up procedures include internal and off-site rotation of electronic files.

Recovery Plans and Tests

The IT Disaster Recovery team develops tests and maintains disaster recovery plans for mission critical applications in the data centers. Exercises are scheduled at least annually to confirm that the applications can be restored properly, that all interfaces are accessible, and timeframes are met. Surprise simulation drills are also conducted to enhance the preparedness of the recovery teams.
Customer Service – Answering the call for operational resilience

Providing industry leading customer service is an important way for us to understand our customer’s expectations, assist with questions, and ensure satisfaction with the services we provide. We continue to invest in our ability to provide excellent customer service, whether the customer contacts us during routine operations or in the midst of a hurricane.

Our customer service operations are designed to be resilient. The contact centers are equipped to adapt to changes in customer call volumes, call types, or other circumstances so that they meet service quality targets. Customers are also provided with many different ways to interact with us. For example, customers can gather information about their accounts using our website and other self-service tools if these are most convenient for them.

Call routing between multiple locations

Our customer service team operates multiple contact centers located across the United States. Our teams can redirect calls between these locations to provide the best service possible and to optimize the skills of our personnel. This operational strategy is a valuable asset during times of crisis, since it helps minimize the customer impact from a disaster that may affect one location. For example, if one contact center needs to close due to a threatening major storm in the area, that center can redirect its calls to an alternate center in an unaffected part of the country. Our national operations infrastructure is a benefit for our customers since it limits the likelihood that any one event will cause a significant impact to our customer service operations.

Contact center infrastructure

We pay particular attention to the design of our contact centers, not only to make them a safe and enjoyable workplace for our employees, but also to minimize the risk of a disruption. These efforts include special security access to the building, including security guards, camera systems, and lighting systems. The communications equipment is maintained in a secure and environmentally controlled computer room, which is supported by both backup batteries and generator power.

Recovery Plans and Tests

Our customer care teams work closely to monitor service levels, and the need to redirect calls to an alternate contact center. We have documented many of these routing patterns in our recovery plans to streamline our ability to activate the technology in the event of an interruption, and to send calls to the teams that are best equipped to help the customer.