**Emergency Planning: First Responders**

**FastLinks**

* [FEMA](http://www.fema.gov/)
* [Ready.gov](http://www.ready.gov/)

Disaster preparedness and recovery planning is designed to reduce the disruption of essential services when an emergency situation occurs. Emergency communications planning is key component of any disaster plan. Disaster plans should be flexible enough to be adapted to particular emergency situations.

The following guidelines are intended to help First Responders ensure their continuity of operations and manage the security and operability of their communications systems and networks during emergencies. You may voluntarily choose to use these guidelines to further develop, enhance and expand their current emergency and disaster preparedness, response and recovery plans to build in a more comprehensive strategic approach to their overall emergency communications plans.

In formulating your plans, the goal is to develop and implement strategies that ensure the continued operation of facilities before, during, and after an incident. Hence, the main steps are ***preparation***, ***response***, and ***recovery***.

**Preparation**

**Communications and Continuity of Operations (COOP)**

* **Operational processes.** Identify those with key communications and information technology (IT) components that are critical to the continuation of essential services in an emergency. Also specify any procedures to be followed in the hours preceding a storm to protect computers, paper records, e.g., securing equipment, placing garbage bags over files, or moving files upstairs. Identify which, if any, databases should be backed up at the last possible moment.
* **Recovery processes.** Develop processes to be used during the recovery. They should include procedures for impact assessment, repair/restoration, alternate solutions, post-incident analysis, and the updating of the emergency management plan. Pre-emergency procurement processes/contracts should be in place with appropriate industry partners/vendors that will enable the rapid acquisition of critical telecommunications equipment/services such as fixed and mobile satellite systems which may not be a capability in daily use by critical entities.
* **Communications response team.** Develop a team that will take action during and following an emergency. This task must clearly define employee roles and responsibilities and establish a chain of command for operational functions and maintenance of communications infrastructure and IT services.
* **Employee training exercises.** Conduct training for all phases of an emergency. Where feasible, consider doing cross training between communications team members to be able to compensate for personnel shortages that may occur. Include specialized training for employees with disabilities and those who work with them.
* **Communications leader training.** Conduct training for those responsible for coordinating communications operations during major emergency events.
* **Employee contact lists.** Develop lists that include office telephone numbers, work cell phone and blackberry contact numbers, and office email addresses. Also include personal home and cellular telephone numbers and personal email addresses. Continually update the lists to ensure that complete and current emergency contact information is on file and accessible. In addition, maintain the lists in paper format and on removable media such as USB drives that are stored off site. Also develop a list of employees with disabilities, giving instructions on how to contact them in an emergency (e.g., how to send a text message to a deaf employee's pager). In addition, develop a plan for how to keep people with disabilities informed in case of an emergency.
* **Service provider contact lists.** Prepare contact information for IT, Internet, and telecommunications services. Include circuit numbers, Diagrams and TSP codes (see below).
* **Priority services.** Three key federal programs are available that allow for priority call queuing and the priority provisioning or restoration of key communications circuits (see Network Reliability and Interoperability Council Best Practice 7-7-1011). The programs are:
	+ [TSP](https://transition.fcc.gov/pshs/services/priority-services/tsp.html), or the Telecommunications Service Priority Program, provides organizations engaged in national security and emergency preparedness (NS/EP) functions with priority provisioning and restoration of telecommunications services that are vital to coordinating and responding to crises. Telecommunications service vendors prioritize service requests by identifying those services critical to NS/EP. A telecommunications service user with a TSP assignment is assured of receiving service by the service vendor before a non-TSP service user.
	+ [GETS](https://transition.fcc.gov/pshs/services/priority-services/gets.html), or the Government Emergency Telecommunications Service Program, provides emergency access and priority processing in the local and long distance segments of the Public Switched Network (PSN). It is intended to be used in an emergency or crisis situation during which the probability of completing a call over normal or other alternate telecommunication means has significantly decreased.
	+ [WPS](https://transition.fcc.gov/pshs/services/priority-services/wps.html), or the Wireless Priority Service Program, improves connection capabilities for a limited number of authorized national security and emergency preparedness (NS/EP) cell phone users. In the event of congestion in the wireless network, an emergency call using WPS will have priority queuing for the next available channel.
* **Alternate operations site.** Such an alternative is essential in times of emergency. The designated location must be able to support critical IT and communications functions.

**Redundant/Back-up Communications**

Assess communication systems in order to determine which systems and/or databases require redundancy.

* Identify and establish safe locations for communications systems that require redundancy and back-up configurations.
* Have a tested backup plan for satellite telemetry and control.
* Perform periodic testing of systems to make sure they will work in an emergency.
* Identify specific vulnerabilities (i.e., power outages, high wind, flooding, etc.) that are most likely to occur in that specific region and provide resources to overcome them.
* Evaluate the resiliency, redundancy, and interoperability of the system while performing your inventory and risk assessment analysis. These steps should consider:
	+ Diversity of communications systems (see below),
	+ Last Mile Connectivity,
	+ Facility Hardening and Alternate Routing,
	+ Internal Building Infrastructure,
	+ Hardware Back-up,
	+ Un-interrupted Power supplies/Internal Reserve Power,
	+ Availability of replacement parts, on-hand and in the market,
	+ Redundant Paths and Physical Routes, and
	+ Switching and packet re-route capabilities.
* Learn the capabilities of the system so as to maximize the value of the plan. If you do not know these systems well and do not use them prior to an emergency, they are likely to fail during a major event due to lack of knowledge or readiness.
* Obtain a last-resort backup means of communication (such as Wireless, WIFI, satellite) in response to adverse conditions, even if technical signal quality is substantially degraded under such conditions, for communicating with employees, police, fire department officials, emergency medical personnel and others in the community as needed.
* Consider HF radio as an option, recognizing that HF usually requires a skilled operator such as a licensed HAM radio operator. It is advisable to identify and include HAM radio operators in your emergency operations plan and when activated, identify where they will be assigned. It is important to include all known HAM, Amateur Radio Emergency Service (ARES), and SHARES operating personnel in the area to maximize their assistance during critical times.
* Preplan when known events are forecasted. This allows you to implement a preparation plan that institutes a procedure for readiness and testing of all frontline and redundant equipment. Preplanning includes topping off fuels, recharging batteries, adjusting work schedules, and notifying standby staff. Make sure all critical communications facilities are on the plan, as well as other private networks that are key in supporting emergency communications operations.

**Diversity of Communications System**

Examine the vulnerability of each communications service provider's infrastructure and facilities and consider the use of alternate providers.

* Periodically test all redundant communications systems.
* Consider the use of divergent routes, such as an office across the street that may be fed from a different cable or transformer. This is best accomplished in a discussion with your telecommunications service provider.
* Even in those cases where end-to-end diversity is not available (perhaps because there is only one loop route to the PSAP), the PSAP should consider obtaining interoffice diversity from its provider.
* The PSAP should also consider arranging with another PSAP for backup and support in the event of total failure or abandonment of the PSAP.

**Emergency Notifications**

Have policies and protocols in place to ensure that all personnel have access to emergency notifications, via various communications devices.

* Consider using a number of notification systems such as building-wide intercom, wireline phone messages, email notifications, and person-to-person communications for crisis management instructions (e.g., for full evacuation or relocation to a designated area of the building.
* Ensure that notification systems can function in the event of a power failure. Although consideration often is given to lighting, public address or other notification systems sometimes are overlooked.
* Identify employees with disabilities and special needs and work with these employees to develop strategies for keeping them informed during an emergency. Some employees, for example, may be unable to see or hear workplace announcements.
* Develop plans for evacuating employees with special needs, such as those in wheelchairs.

**Security**

Secure communications and IT systems/facilities from physical and cyber attacks.

* Maintain vital communications and IT equipment in protected locations with only authorized access.
* Secure key facilities with experienced personnel and/or video surveillance cameras.
* Limit access to IT systems to appropriate staff using login/password and other security measures.
* Protect communication and IT systems from malicious cyber attacks and viruses by implementing security measures such as the regular updating of virus protection and other software security programs.

**Power**

Have plans in place that account for commercial power disruptions for extended times during and following an emergency. Actions to take:

* Activate backup power automatically through the use of a power source having a low risk of being interrupted during a power outage to maintain continuity of operations (i.e. a power generator).
* Deploy power generators at secure, elevated locations in cases where it is essential to maintaining daily operations. Generators should be maintained by frequently testing them.
* Ensure that sufficient levels of fuel are available at all times and periodically check those levels. When ordering a new installation, consider using dual fuel, such as Natural Gas and Diesel.
* Ensure that power batteries are available for critical communications in case the power generators fail to function. Consider installing solar power or fuel cells where applicable. It is important to note that batteries are good for short term outages but often do not power the air conditioning equipment and do not adequately cool the other equipment (especially computers) which may be damaged or shutoff when overheated.
* Consider purchasing new radios that can be powered by off-the-shelf alkaline batteries using appropriate adapters. Note, however, that batteries are only short term fixes and are depleting commodities that present a HAZMAT issue in disposal. Moreover, they will not power critical HVAC and environmental systems necessary for the operation of your facilities.
* Establish sources for obtaining fuel to refill generators.
* Make sure that batteries for radios, flashlights, fire detectors and other communications and safety devices are working, charged, and ready. Develop a daily, weekly or monthly schedule for periodically testing them.
* Keep additional supplies of batteries at the worksite and at the alternative operational site. Rechargeable batteries should be tested in appropriate equipment and replaced periodically based on manufacturers' requirements.

**Test Equipment**

Verify the availability of technician test equipment that may be needed when an emergency occurs. Also verify that test equipment works with both commercial and battery power when applicable.

**Mutual Aid Agreements**

Enter into mutual aid or lend-lease agreements with similar organizations inside and outside of your area. In some cases, these agreements will enable organizations to share specialized resources rather than duplicate them in every jurisdiction.

* Work with local public utilities (e.g., telephone, wireless phone, electric, and water) to develop a critical infrastructure priority restoration plan for your locality.
* Establish a procedure and determine "emergency" contact telephone numbers with each of these agencies.
* Meet and get to know these critical players before the need arises.

**Things To Consider**

**Response**

Activate the ***Emergency Response Process*** which includes procedures for impact assessments, repairs and implementation of alternate communications solutions. Entities should:

* Contact and bring together emergency staff members to brief them on response tasks.
* Complete a communications system assessment to determine the operational status of your various communications systems: land mobile radio system, repeaters, PBX, LAN or data network, and email (incoming, outgoing, and internal). During the assessment, examine the following areas:
	+ Inventory of assets, in use, in maintenance, on loan, and in back-up;
	+ Infrastructure maintenance, performance against standards, system saturation, usage, and traffic loads;
	+ Current Disaster Recovery Plan;
	+ Current emergency support personnel;
	+ Current Service Level Agreements and response time from vendors;
	+ Current priority of service on all forms of service provided;
	+ Communications and system repairs;
	+ Current network resiliency, redundant paths, and primary/secondary fail over systems; and
	+ Most current vendor, service provider, and State and Federal contacts.
* After establishing what is in inventory and available, determine the level of support the system can give you. Establish a three-tiered priority list that will help you know the impact of losing a given asset and will allow you to better communicate your needs for assistance when necessary. Three levels of criticality are commonly used:
	+ ***Mission Critical*** indicates a catastrophic breakdown in response ability which could result in major loss of life, property, and system trust breakdown. This situation requires an immediate effort to target restoration.
	+ ***Important*** indicates a severe decrease in the ability to respond to emergency needs. There could be excessive loss of life or property associated with this type of outage. Only critical responses could be met.
	+ ***Minor*** indicates that full capabilities could be apparent to the public with modifications to the systems and its architecture or software.
* Perform a communications line assessment to determine the operational status of telecommunications lines connecting your organization to the outside world.
	+ Activate backup systems to compensate for failed communications systems or lines and make sure that the backups have kicked in.
	+ Complete repairs of those communications systems that the IT/telecom department can repair on its own. In addition, contact commercial vendors for repairs (including telephone companies if any of their lines or services have been impacted by the emergency).
	+ Conduct situational awareness surveys/analyses and provide updates and reports to the organization's leadership and emergency management team, and, when appropriate, to the public.
	+ Develop risk modeling against your first responder infrastructure and your response, based upon the top disasters your area is prone to. The analysis should run the gauntlet of issues including total loss of systems.
	+ Use inclusions that test fail over for lost facilities, loss of human services, current structure and building designs, tower locations, and [National Institute of Standards for Technology](https://transition.fcc.gov/fcc-bin/bye?http://www.nist.gov).
	+ Perform an analysis that includes a steady and repeatable result and allows for a gap analysis of the systems and their functions. Areas of single point of failure should be identified and prioritized as tactions mitigating the impact of failure.
	+ Include studies of current design and standards, as well as recovery based upon current service level agreement response intervals.
	+ Also include the cost associated with the infrastructure, system, and personnel loss, as well as a mitigation study of liability impacts and supplemental loss.

**Things To Consider**

**Recovery**

Activate the Emergency Recovery Process which includes procedures for conducting impact assessments, making repairs or restoration, establishing alternate solutions, performing post-incident analysis, and updating the emergency management plan.

* Develop a means of personnel identification to insure access during these critical times. Do the same for any mutual aid agencies that may be helping.
* Contact and gather emergency staff to review impact assessments to complete repairs and restoration of communications systems.
* Complete a communications system assessment to determine the operational status of communications systems such as PBX, LAN or data networks, and the incoming, outgoing, and internal email system.
* Perform a communications line assessment to determine the operational status of telecommunications lines connecting your business to the outside world.
* Conduct an IT system assessment to determine the operational status of key computer systems for continuity of operations.
* Complete all repairs and a post-incident analysis and utilize a lessons learned approach to emergencies.

Update the organization 's emergency management plan as necessary. Schedule post-incident follow-up meetings and drills to address any outstanding emergency preparedness, response and recovery issues within 60 days of the incident.

* Consider holding a debriefing session with employees or visitors with disabilities or special needs to determine how well emergency procedures worked for them and what, if anything, can be improved.
* Remember that **failing to plan is planning to fail**.