Why communications planning is key to emergency management

A guide to effective communications planning in the public sector (with real-world examples)
Introduction
The foundation of a good response

Whether it’s a police officer attending the scene of a crime, an EMS team rushing towards a major accident, or the FBI swooping in to preserve national security, when we think of first responders, we think about exactly that—response.

But dealing with emergencies well isn’t just about reacting—it’s about planning, training, mitigating and exercising. Repeatedly. Deliberately. In a way that’s continuously improving.

In the past, communication was considered the fifth or sixth order priority in emergency management planning.

But in a post-9/11 world, the onus on every team involved in emergency management is to share information, establish accountability and operate transparently.

Which makes communications one of the biggest priorities.

In practice, the right communications infrastructure and systems can make a very real difference between life and death.

This guide explores why the most proactive agencies and organizations prioritize communications planning when they’re preparing their emergency management protocols and provides essential context for devising a plan of your own.
Where communications plans fit into standard emergency planning
Where communications plans fit into standard emergency planning

All-hazards planning

Today, almost every practitioner takes an ‘all-hazards’ approach to emergency response planning.

This approach, which underpins the National Incident Management System, responds to a simple fact: the modern world contains so many potential threats, trying to predict which an agency will face at any given time is extremely challenging, if not outright impossible.

In an All-Hazards approach, all known hazards and vulnerabilities are documented, their likelihood of occurrence is measured, and their impact on operations is analyzed.

With this approach, risk mitigation and contingency plans are developed through the Threat, Hazard Identification and Risk Assessment (THIRA) process.

Of course, it’s impossible to know every threat, or to forecast with absolute confidence when it might occur, or what its impact may be.
Incident Action Planning tackles the planning challenge at the level of the individual response operation, documenting the tactics needed to meet the overall goals or ‘control objectives’. Those tactics may include search and rescue, a surgical extraction, or the creation of a temporary Joint Operations Center for a specific event (like an active shooter or dangerous weather).

The resulting Incident Action Plan (IAP) provides a basis for coordinated response activity, becoming the key tool for overall incident management. IAPs include many elements, but among the most important is the Communications Plan.

The Communications Plan must look at a broad array of topics both prior to and during an incident:

- Pre-planned and evolving incident-specific requirements
- Interoperability needs
- Access to information and situational awareness
- Available Primary, Secondary and Tertiary resources

Primary resources are those chosen to provide the highest degree of reliability during normal operations. Secondary resources are those chosen to mitigate the impact of a communications failure. And tertiary resources—often taking the form of “resource playbooks”—deepen an agency’s ability to meet almost any need, during any event.

Last but by no means least, the Communications Plan must support the development of coordination and collaboration between both responding entities and the resource partners supporting response operations.

As commercial LTE and traditional public safety systems converge and technology seemingly advances at a much faster pace than adoption, understanding the communications environment responders will face is key.
Planning for challenging communications environments
What does an Atlantic hurricane have in common with a murder in rural Virginia?

Both left response teams in incredibly challenging communications environments. And both prove that without effective communications, it’s impossible to effectively coordinate an emergency management operation. Whether it’s a clean-up or a manhunt. Whether you’re city firefighters or national law enforcement officers.

Let’s look at these challenging communications environments and talk about preparations for each.
Planning for challenging communications environments

Comms environment #1
The network has been damaged

Often the very emergency you’re managing will take a toll on the communications network.

Creating a robust emergency communications plan means knowing how you’ll re-establish the coverage you need. Will you seek to quickly replace the damaged infrastructure? Or ‘ghost’ it with temporary equipment that does the same job?

Back in 2011, Hurricane Sandy caused both wireless and wired networks to shut down on the shores of Southern New Jersey, through New York, and up to the Western Great Lakes.

Sprint deployed its SatCOLT fleet more than 47 different times supporting field operations such as search and rescue, security operations, joint field operations, disaster recovery centers, and joint staging facilities (just to name a few).

Unique to the Hurricane Sandy response was the very dense urban environment, with its extremely tall buildings and underground network infrastructure. This meant that, when Emergency Operations Centers were activated, they were located in places with connectivity issues—such as the 32nd floor of 50-story buildings.

The surge in response personnel into this particular EOC far exceeded the planned capacity of the facility, overwhelming the already impaired telecommunications infrastructure.

Satellite communications were the only solution. But rolling out the necessary support infrastructure on the ground was not an option. The only option then was the roof, but still some 18 floors above the EOC. Rising to the challenge, Sprint ERT personnel solved this problem, deploying Satellite Fly Away Antenna Systems on the roof of the building, some 18 floors above the EOC and running fiber through cable chases and elevator shafts.

With the extra capacity, command operations could resume. EOC staff were able to access situational awareness such as GIS and WebEOC, conduct coordination and planning operations, and communicate with other response personnel and the public at large.
Planning for challenging communications environments

Comms environment #2
There’s insufficient interoperability

Even if the network remains uncompromised, achieving effective communication can still be a challenge.

In any Mutual Aid scenario, where first responders from multiple jurisdictions and agencies need to work together to achieve a larger goal, a lack of interoperability in communicating systems can present a huge barrier to success.

Remember the manhunt we mentioned earlier? It took place across two different counties, over two different radio networks. Not only did local law enforcement respond, so did federal, state and other jurisdictional agencies. In fact, over 200 law enforcement officers were dispatched into the field for the manhunt each day for three days straight.

The two county Land Mobile Radio (LMR) networks spanning the county lines weren’t connected. The radio equipment resources brought in by the responding mutual aid agencies didn’t talk to each other. Simply put, there wasn’t the interoperability needed to coordinate using radio comms.

The command post was established at a local church, far from any terrestrial or wireless broadband. It was exactly the kind of scenario where a Communication Unit Leader needs to leverage their playbook of resources and rapidly plan a response that can solve multiple problems at once.

In this case, deploying a Sprint ERT SatCOLT was key. With a radial coverage footprint of up to 5 miles, the SatCOLT provided much-needed connectivity in the valleys of the Virginia mountains. Meanwhile, over 300 Sprint Direct Connect handsets provided connectivity across and between agencies. Operating just like an LMR system, it provided command staff secure one-on-one communications, while task force leaders could communicate via talk groups within and across the units tracking the suspect.

At the command post, Sprint’s Emergency Response personnel engineered and deployed secure, local area networks. These networks were connected to Sprint’s global IP backbone via the Sprint ERT satellite network using ERT’s mobile IP trailer system.

With connectivity in place, unified command could coordinate effectively, and agencies could access tracking systems and conduct aerial search operations, while also keeping the public informed through on-site media.

How a lack of interoperability creates a single point of failure.

Improving interoperability doesn’t just solve the problem of connecting disparate networks and applications; it allows for diversity, and as a result, redundancy.

Without interoperability, agencies wishing to talk and share information with each other would be forced to use one network, one system, one radio type. This would leave Public Safety and Emergency Management professionals with a single point of failure, in environments where failure is not an option.
Planning for challenging communications environments

Comms environment #3
There’s little or no network coverage

Some parts of the US remain much better connected than others. If there’s a possibility you’ll need to manage an emergency where network coverage is poor or non-existent, it’s important to factor this into your plans.

For example, the emergency personnel who responded to the Upper Big Branch Mine Disaster in West Virginia quickly discovered that communication was limited by the rural location and the local topography.

Coverage for cellular and land mobile radio was not sufficient to connect these first responders. What’s more, due to the hazards, and a toxic airborne environment, staging and decontamination had to occur a safe distance away from the mine. This distance severely impacted search and rescue operations.

Incidents regularly occur in contexts like this—where Public Safety and Commercial networks don’t exist, or can’t support the scale of response operations.

In such cases, deployable infrastructure is often the only solution. For example, Sprint SatCOLTs can provide a 3 to 5 mile bubble of LTE and Cellular coverage. And Sprint’s Emergency Response Team solves interoperability concerns by also deploying the necessary communications equipment, such as Push-to-Talk smartphones that are ruggedized against wind, rain, smoke, and dust.
03

Factoring in local geography and likely timescales
Factoring in local geography and likely timescales

Depending on the location and mission of your organization, you may need to respond to a range of events, in a diversity of communications environments.

As we’ve seen, your communications plans don’t need to detail every potential emergency management scenario. But the provisions you make should reflect the challenges you’re most likely to face based on the local geography, as well as the amount of notice you’re likely to get before the emergency begins.

Geographical considerations

In Florida, an organization might well plan how to ensure communications when responding to hurricanes and tornadoes. In Missouri, they might spend more time on earthquakes and flooding. And in the West, wildfires may be high on the agenda.

If you’re based in a rural area, you’ll want to check network coverage carefully whatever your organization’s responsibilities, and put mitigation strategies in place.

In major urban areas where network failures impact much larger population bases, achieving coverage and connectivity may be impaired by dense infrastructure. Manmade threats—like coordinated terrorist activities—may also be more likely.
Factoring in local geography and likely timescales

Time considerations

There’s another useful way to think about the type of emergency communications scenarios you might need to manage: how much warning will you have?

With an attack by a bad actor of any sort, there’s usually little to no notice that your emergency communications plan needs to spring into action. The same is true with flash flooding.

With a hurricane, however, there may well be advance warning—and a greater window in which to prepare any emergency communications measures. This extra time to ready your response could influence the type (and ownership model) of the resources you include in your plan.

Sometimes it’s the team you rely on, not the equipment.

Following the acquittal of St. Louis Police Department (STLPD) officer Jason Stockley, STLPD decided to set up a temporary command post in order to monitor the evolving protests, and provide immediate local support in the protest area.

The location was an abandoned facility where no internet access existed and in-building wireless service was limited for all carriers. To complicate matters, operations needed to launch at the command post in less than 24 hours.

Understanding the importance of the situation, Stephanie Tobar, a Sprint ERT Reservist and account manager for St Louis Police immediately leapt into action. After a brief planning meeting with the customer, a task force was created; Sprint’s Emergency Response Team was selected to lead the response.

Less than three hours later, the task force of 10—representing eight different fields of technical expertise—had convened. They created an Incident Action Plan, presented it back to the police department, and made arrangements to begin work.
Keeping your emergency comms plan up-to-date
Keeping your emergency comms plan up-to-date

As we’ve seen, creating an emergency communications plan is a vital part of robust emergency response planning. Reviewing your plan regularly is just as important. Most state and federal organizations review their emergency comms plan on an annual or biannual basis. You may however, choose to review yours at a difference cadence depending on your specific circumstances.

The most effective planners reach outside their own jurisdictions and areas of expertise to seek guidance from as many expert stakeholders as possible. (Sprint regularly provides such advice and has supported planning efforts including The Regional Catastrophic Private Sector Integration Plan and the Joint Missouri/FEMA Region VII New Madrid Response Operations Plans.)

Conducting a regular review will help you ensure your plan stays aligned to your needs, and the emergency scenarios you face, as both evolve over time.

It’ll also ensure you’re considering how communications technologies are changing, and know the cost, performance and functionality opportunities they represent.

Here are some of the emerging technologies you’ll want to consider.
Emerging technologies and applications

Saving responder lives with 5G

5G’s lower latency (and higher capacity and throughput) is set to transform the safety of first responders—allowing command staff to remotely monitor their vital signs, temperature, and even whether they’re moving freely, or lying prone on the ground.

Empowering dispatchers with UAVs and the IoT

Imagine there’s a building fire in the middle of a smart city. With UAVs, it’s becoming possible for a dispatcher to gain a bird’s eye view of the incident. And if the building’s HVAC system is part of the IoT solution, they can even see where the temperature is rising fastest.

5G reduces the delay between control inputs and the UAV response, increasing agility and allowing dispatchers to get exactly the view of the fire they need. It also enables the UAV to transmit far more data from their cameras or sensors. (Very high definition video, which increases situational detail, becomes more feasible with 5G.)

So does outfitting that UAV with thermal sensors or night vision equipment.)

All this means the first responders have the information they need to make the right response decisions, without the delay or risk to life of sending a human to investigate.

Keeping your emergency comms plan up-to-date

Emerging technologies and applications

Sprint Business  Why communications planning is key to emergency management
Keeping your emergency comms plan up-to-date

Emerging technologies and applications

Enhancing planning with 5G and IoT

As we’ve seen, planning for an emergency response scenario is really about trying to consider all the possibilities. And with the data that 5G and IoT will soon deliver, those possibilities become probabilities.

For example, insights from sensors placed on key infrastructure components—e.g. road bridges—will help planners better understand the traffic they would be able to cope with in an emergency scenario.

Improving communications coverage with UAVs

UAVs also provide another way to establish communications coverage in areas where infrastructure is lacking. Fly a UAV with the right radio equipment into an area hit by forest fires, for example, and you can create an extended area of strong wireless coverage—invaluable to firefighting personnel on the ground.
Communication is the backbone of any successful emergency response operation.

It’s the difference between siloed efforts and coordinated action. Between best guesses and informed decisions. Between lives lost and lives saved.

And ensuring effective communication is possible, whatever the circumstances, takes careful planning.

If you would like help assessing your emergency communications needs and strategy, please contact the Sprint Emergency Response Team 24x7x365 at:

**Toll Free:** (888) 639-0020  
**GETS Users:** (254) 295-2220  
**Email:** ertrequests@sprint.com

Conclusion
What can you do now to save lives later?
Let’s talk

We’re Sprint Government. And we’ve been protecting First Responders with public safety solutions for more than 30 years. So if you’re looking for reliable emergency response communications in an emergency, get in touch.

Talk to us about our emergency response solutions.
Call Toll Free: (888) 639-0020
GETS Users: (254) 295-2220
email: ertrequests@sprint.com or see more details on government.sprint.com/publicsafety