The value of smartphones and handheld devices for government Continuity of Operations (COOP) and emergency response

Executive summary

Communication and ready information access are the keystones of effective government services. Never are they more urgent than when normal operations are disrupted—for example, by hazardous materials spills, accidents, weather, contamination, attack, or pandemic. During these and other emergencies, local, state, federal civilian, and federal defense agencies must coordinate their activities and follow operational procedures to save lives, minimize property loss, protect the environment, and achieve a timely and orderly recovery to normal operations.

Smartphones and other handheld devices support government continuity of operations (COOP) by enabling its central tenets: decentralization and redundancy. Decentralized command and control becomes possible when government employees and public safety personnel can communicate and access vital information from the field as readily as if they were at their desks. Redundant communications options for smartphones—voice, short message service (SMS) text messaging, and email over cellular, WiFi, and satellite networks—enable uninterrupted communications and information access even if one network becomes unavailable.

The value of smartphones also extends to day-to-day government operations. For example, first responders can use smartphones to query law enforcement databases. Emergency medical services (EMS) personnel can access drug formularies to prevent adverse drug reactions. Field personnel can receive real-time alerts from sensors such as access control systems or air-quality monitors, helping to ensure a timely response. City inspectors can upload and access building and site information, such as potential hazardous materials, for faster approvals or interventions during annual inspections

This white paper discusses the value of smartphones and handheld devices as part of government COOP and emergency response strategies. The first section reviews COOP challenges, including the limitations of ordinary cell phones, laptops, and the public switched telephone network (PSTN) during emergencies. The next section describes smartphone solutions that enable government to continue delivering services during emergencies or disruptions. The white paper concludes by describing characteristics of smartphones that maximize their value for COOP and emergency response.

Contents

COOP challenges in federal, state, and local government

Types of events requiring COOP capabilities include acts of nature, such as fire, flood, and inclement weather; accidents; technological emergencies; terrorist attacks; and localized incidents such as hostage situations, suspicious packages, or contamination. Another event of growing concern is avian flu or other pandemics, which are expected to disrupt normal government operations because many public and private sector employees will be directed to work from home to minimize disease transmission.

COOP planning requirements

The following factors complicate COOP planning:

- *Communicating with a distributed workforce.* The Washington D.C. Emergency Management Agency, for example, has 65 separate facilities in the D.C. area, and approximately 20% of its employees are mobile.
- *The urgency of rapid information dissemination.* A jet flying at a relatively slow speed of 200 miles per hour can reach the Capitol Building within eight minutes of entering the no-fly zone. Therefore, government needs the ability to very rapidly issue evacuation orders or other directives to hundreds or thousands of government employees.
- *The inability of first responders to know each others' locations.* Even if incident commanders at headquarters know the location of field personnel, field personnel themselves generally are unaware of the location of other personnel, sometimes preventing a coordinated response.
- *Lack of situational awareness.* First responders typically have the most thorough situational awareness—for example, the nature of fires or chemical spills, wind direction, plume direction, or the size of a crowd to be dispersed. Relaying this information to other first responders or incident commanders is challenging with voice systems alone.

Limitations of today's communications devices and networks for COOP

Laptops, cell phones, and the PSTN all play useful roles in government COOP strategies, but each has its shortcomings for various types of emergencies.

Laptops untether government employees from their desks, allowing them to access information from any location with a network connection. They also enable telework, an essential part of COOP strategies. Their weight and bulk, however, make them impractical for employees on the move, such as law enforcement personnel on foot patrol or motorcycles, or urban search and rescue personnel who need to access medical and safety procedures as they extricate people trapped in tight spaces. Other limitations of laptops for COOP are their relatively short battery life and lack of ubiquitous connectivity. Without a separate cellular account for their laptop, employees can connect only when within range of a WiFi network.

Traditional cell phones have proven useful for everyday government operations. An incident commander who is outside of radio range when an incident begins, for example, can communicate with the dispatcher. During emergencies, however, cell phones provide limited value. They are impractical for data-enabled applications and do not provide adequate on-board storage for documents such as orders of succession or operational procedures.

The PSTN—still the mainstay of communications during day-to-day government operations—cannot be counted on exclusively during emergencies. High call volume or equipment damage can result in inacessible or congested circuits, as demonstrated during 9/11 and Hurricane Katrina.

COOP requirements from FPC 65

- Ensure the continuous performance of an agency's essential functions/operations during an emergency or situation that disrupts normal operations
- Protect essential records
- Reduce loss of life, minimize damage and losses
- Achieve a timely and orderly recovery from an emergency and resumption of full service to customers
- Ensure interoperable communications

The role of smartphones in COOP planning

Smartphones and other handheld devices support the myriad forms of communications—voice, text, database access, images, and streaming video—that government employees need for situational awareness and effective response during emergencies (Figure 1). The form factor is small and lightweight, suiting smartphones for many types of emergency conditions. Recent advances in cellular networks provide increased reliability and resilience.

Figure 1 - Converged voice, data and data on a single device

With a wireless connection, smartphones and other handheld devices can contribute to COOP capabilities by enabling:

- Incident management, threat-level management, and emergency alerts
- Incident reporting
- Messaging: inter- and intra-agency communication
- Secure access to critical databases for decision-making
- Enhanced situational awareness through alerts and streaming video
- Smartphone document storage
- Communications resilience
- A Common Operational Picture (COP)
- Telework, if the office is uninhabitable or roads are impassable

Why now?

Today's 3G cellular networks, with their much higher data rates, enable transmission of video and images to smartphones with high-resolution displays, enhancing situational awareness. In addition, cellular carriers now provide capabilities that make their networks resilient and available, including:

- The ability to deploy portable radio towers
- Wireless Priority Service (WPS) that gives priority to calls from or to pre-identified government employees
- Hot switchover to other bandwidth if the network becomes saturated during an emergency
- Vehicle-mounted Global System for Mobile Communication (GSM) or Code Division Multiple Access (CDMA) base stations that can maintain cellular as well as satellite links while the vehicle is moving

Integrated incident management, threat-level management, and emergency alerts

> "In the past, sending a message blast from the field about an incident would require my finding a laptop and WiFi hotspot. Using my Palm Treo, I can access the Web from any location to instantly notify 400 government employees and 100 private-sector individuals about an emergency."
>
> Sheriff Ricky Edwards, Director,
> Office of Emergency Preparedness,
> Jefferson Davis Parish, Louisiana

An effective COOP plan requires rapid incident reporting—for example, informing government building occupants as well as first responders that a suspicious package is in the lobby. The shortcoming of many emergency alerting systems is that message distribution takes too long. Some employees are notified by phone, others by email, and others via text messaging—and each form of communication requires a separate action that can postpone receipt of the incident report or message.

Note that some of the above capabilities require third-party software.

Third-party solutions for smartphones enable an agency manager or incident commander to issue one message and disseminate it instantly to all devices that agency employees use, including smartphones (Figure 2). The agency manager can save more time by using the smartphone's touchscreen to select pre-formatted messages such as "Shelter in Place" or "Evacuate Immediately." The person who sends the alert can also automatically receive a headcount of all recipients who confirmed that they received the message, helping to protect employee safety.

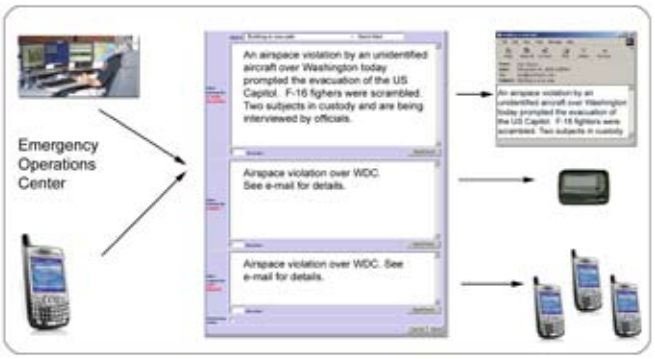

Figure 2 - Smartphones can send and receive emergency alerts

Agencies can also use smartphone solutions that integrate incident management, threat-level management, and emergency alerts. An employee who sees a threat such as an unattended package in a building lobby can enter it on the smartphone, noting the building location and category of incident. Alerts can also be generated automatically—for example, from video surveillance cameras with motion-analysis software or from sensors for building access controls, air-quality monitoring, and so on.

Agency managers carrying smartphones receive alerts quickly, as SMS text, video, voice, or e-mail. If authorized, they can change the threat level, which automatically changes the security procedures for field employees and notifies them by text message. For example, during a red threat level, employees who typically open a particular door at 8:00 a.m. might be instructed to not open it at all—and also to check briefcases and purses for people entering through other doors. Disseminating emergency procedures to employees' smartphones within seconds of the incident report helps ensure that employees follow procedures even if they have not had recent training.

The complete event-response process—reporting, alert, and distribution of new security-posture instructions—occurs in seconds, accelerating response and therefore increasing the likelihood of a positive outcome.

> "Previously, officers waited up to 10 minutes for dispatchers to reply to queries over the radio, but with our new handheld system, response times average two to four seconds for inquiries. This saves valuable time, especially during emergencies."
>
> Marcia Harnden, Law Enforcement Officer,
> City of Bellevue Police Department,
> Bellevue, Washington

Use scenario: Emergency alerts
The Office of the Chief Technology Officer of the Government of the District of Columbia plans, develops and implements the use of new technology for more than 80 agencies, including emergency management and the police department. A tactic in the DC government's COOP strategy is the Citywide Messaging Program. Government employees can send out emergency notifications to key city leaders and personnel in the event of a disaster, attack, or impending incident, enabling faster response. Instant wireless communications to workers in any location is a critical component of the district's business continuity plan.

Inter- and intra-agency communication

Response to incidents such as hazardous material spills, weather-related disasters, and terrorist attacks typically require a multi-agency task force. Most often, the agencies that participate in the task force use incompatible radio systems. Smartphones, preprogrammed with agency task members' names and phone numbers, can be easily deployed to augment radio systems, ensuring that all task force members can communicate.

First responders and other government employees can also use their smartphones to exchange SMS text messages. SMS is preferable to voice for relaying certain types of information. Sending a street address by SMS, for example, avoids the risk that the numbers could be misheard, and also enables the recipient to refer to it later. During emergencies, SMS might be the only way that first responders can communicate. The reason: every voice call requires a low-latency, dedicated channel between the two callers, and available channels can be used up quickly during emergencies. SMS messages, in contrast, do not require a dedicated channel because they are small and latency-insensitive. Additionally, SMS messages are isolated in the network control channel and are often unfazed by heavy traffic or adverse conditions that can overwhelm wireless networks. During 9/11 and Katrina, for example, first responders were able to use smartphones to exchange directions and other information with SMS.

Use scenario: Intra-agency and inter-agency communication
Establishing phone service in a temporary incident command center can take hours or even a full day—time that cannot be spared during emergency response. When an incident occurred in *Jefferson Davis Parish, Louisiana* over an Easter weekend, the sheriff's office relied exclusively on Palm Treo smartphones until data lines could be established, using them to perform driver's license and background checks on suspects. Officers also used their Palm Treo smartphones during Hurricanes Katrina and Rita in 2005. Although cellular phone service was spotty, officers communicated reliably with text messages and e-mail. Each day the agency director would download Excel spreadsheets containing warrant lists and stolen car reports to his officers' Palm Treo smartphones.

Use scenario: Access to critical databases for emergency response
In the aftermath of Hurricane Katrina, members of the *Duke Trauma Regional Advisory Committee* of Durham, North Carolina, used Palm handheld devices running WISER, a free database containing information from the Hazardous Substances Data Bank (HSDB), which is a toxicology data file from the National Library of Medicine. WISER identifies the effects of chemicals in air, water and food so that medical personnel can administer appropriate treatment.

Secure access to critical databases for decision-making

> "Mobility tools like Palm Treo smartphones with the WISER application serve to shorten critical response time in crisis situations and provide accurate authoritative information."
>
> Lieutenant Chip Haake,
> Tuscola Fire Department,
>
> Tuscola, Illinois

Whether during emergencies and disruptions or day-to-day operations, government employees need access to critical data from locations other than their offices. Today, various federal and local agencies use smartphones to wirelessly access databases such as the National Crime Information Center (NCIC), Criminal Justice Information Systems, and Nlets, the International Justice and Safety Information-Sharing Network, over the cellular network.

Databases can also be stored securely on the smartphone itself, either using on-board storage or a removable Secure Digital (SD) card. Available third-party databases include Wireless Information System for Emergency Responders (WISER), hazardous materials databases, and emergency medical procedures (see sidebar). WISER can either be installed on the smartphone or else accessed wirelessly over the Internet.

Enhanced situational awareness through alerts and streaming video

Increased situational awareness at incident scenes helps avoid loss of life—for citizens as well as first responders—and facilitate a more timely and orderly recovery. Smartphones with high-quality displays enhance situational awareness by delivering images and videos to first responders and incident commanders. The capability was demonstrated in October 2006, when a cameraman for a major news network reported live from the scene of a plane crash in New York using a Palm Treo smartphone installed with software that can transmit streaming video even over non-3G networks, using much less bandwidth than would normally be needed.[1] Similarly, in an emergency such as flooding, first responders can use their smartphones at an incident scene to capture and transmit images or video—of levee damage, for example—to the command center.

[1] Reuters, "Fox Uses Treo to Break N.Y. Plane Crash News," October 13, 2006

Smartphone document storage

"The… ready availability of electronic and hardcopy documents, references, records, and information systems needed to support essential functions under the full spectrum of emergencies is another critical element of a successful COOP plan"

FPC 65

Often, an agency's operational plan is stored in a binder on employees' desks, where it is inaccessible if the employe cannot work in the office because of attack, building contamination, road damage, or pandemic. Employees using smartphones with gigabytes of on-board storage can access the plan of operations no matter where they are—improving agency effectiveness. For COOP planning, critical information that is useful to store on smartphones includes emergency plans and d irectives, delegations of authority, official personnel files, property management and inventory records, and emergency medical procedures. Documents can be encrypted to prevent unauthorized access.

In addition to using their smartphones to store COOP documents, employees can use them to run specialized calculators that facilitate decision-making during emergencies—for example, to calculate a bomb's damage zone and radioactive fallout zone based on wind speed and direction, height of explosion, and other factors.

"I can store everything I need on my Palm handheld computer and a removable SD [Secure Digital] card and take it with me."

Mark Hall, Communications Leader
Incident Management Team,
Jefferson County, Colorado

Common Operational Picture (COP)

At incident scenes, agency task force members often lack information about each others' locations or expected arrival time, inhibiting decision-making and effective response. Typically, only the incident commander is aware of location information for all field personnel.

Specialized mapping software transforms smartphones with high-resolution displays into tactical devices that provide a common operational picture (COP). Public safety personnel and other response teams can use their smartphones to view a map of the incident area superimposed with symbols showing the location, identity, and status of all other task force members—zooming in or out to view the entire affected area or a few square feet. Field personnel can view and indicate the location of fires, spills, individuals needing rescue, or indicate the direction of a contaminant plume.

The COP solution addresses a shortcoming of radio-only communications for emergency response. That is, it is far easier to indicate and view location information on a graphical interface than to describe it on the radio. Using a smartphone with a touchscreen display also makes it unnecessary to type anything other than free text messages. Response time is faster because field personnel can communicate more easily, simply touching the symbol representing another person to initiate a cellular call, send a preformatted message such as "Officer down," or push images or video clips.

Communications resilience

"When identifying communications requirements, agencies should take maximum advantage of the entire spectrum of communications media likely to be available in any emergency situation."

FPC 65

Smartphones enable connectivity over multiple types of networks—an important capability when one or more networks might be damaged (Figure 3). Federal employees equipped with a smartphone can:

- Connect via cellular voice and data networks
- Connect via WiFi, using a third-party accessory, if the cellular network is down
- Connect via satellite
- Use the smartphone as a cellular modem for a laptop, enabling laptop connectivity even if a WiFi connection is unavailable

Figure 3 - Redundant communications options

During disasters and emergencies, government employees also need resilient communications if any element of the agency's email or messaging infrastructure fails: email server, network equipment, or enterprise carrier gateway. Failure of any of these components can prevent government employees from quickly communicating with command and control centers.

Agencies can protect their ability to communicate, despite infrastructure failure, by deploying a third-party emergency-access gateway in an alternate facility (Figure 4). The gateway enables employees to use their smartphones to access vital documents even if the agency infrastructure becomes unavailable.

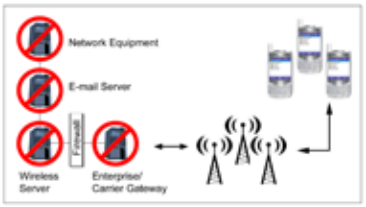

Figure 4a - Infrastructure failure can prevent communications

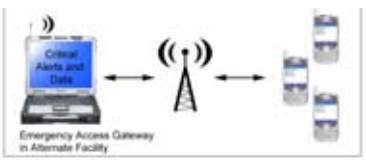

Figure 4b - An emergency access gateway enables critical messaging despite infrastructure failure

Workforce resilience

Empowering government employees to work productively from home is a vital part of COOP strategies. Why? The most resilient network and systems possible are useless if the workforce cannot access them because they cannot enter the building. And yet, conditions such as building damage, anthrax contamination, impassable roads, or quarantine during pandemics can prevent employees from commuting to the office. For government services to continue, employees need flexible, secure access to database information and the ability to create and review documents from home or other locations.

> "Using a Palm Treo device with Windows Mobile software, federal workers can access mission-critical applications while away from the office. A decentralized workforce helps meet COOP requirements and protect vital national interests."
>
> Randy Siegel, Enterprise Mobility Strategist, U.S. Federal Government, Microsoft Corporation

Agencies typically provide laptops for telework. If the budget does not permit providing all employees with laptops, handheld devices with integrated operating systems provide a cost-effective alternative (see sidebar).

Saving valuable seconds in emergency response

Government employees can often send or view critical messages more quickly with a smartphone than a laptop. To send an e-mail from a laptop, for example, the employee needs to turn it on, wait for the operating system to load, and connect to the VPN—a process that can take several minutes. Sending an e-mail from an instant-on smartphone, with its mobile-optimized operating system, takes just a few seconds. The time savings can make the difference for COOP objectives such as saving lives, minimizing property loss, and protecting the environment.

Mobile device solution criteria for COOP

Table 1 lists smartphone characteristics that are especially useful for COOP applications.

Smartphone characteristic	COOP capabilities it enables
Touchscreen display	Rapid communications: employee can initiate a cellular call or send a text message by tapping an on-screen button instead of stopping to dial Rapid information retrieval: using WISER, for example, employee can quickly tap hazardous substance names instead of using a scroll wheel to navigate through a menu hierarchy
Secure onboard storage	Ready availability of essential documents such as emergency plans and directives, orders of succession, delegations of authority, and staffing assignments
Flexible connectivity options: cellular, WiFi, satellite (with portable ground-station terminal)	Resilient communications
Longer battery life than that of laptops	Use in the field for extended periods or when electricity is not available
Support for voice commands	Saving vital seconds at emergency scenes by enabling first responders to open a hazmat or other database or dial a phone number with a spoken command

Table 1 - Evaluating a smartphone or handheld device for COOP

Another important smartphone characteristic is information security, which can be provided by third-party solutions. Loss or theft of mobile devices is inevitable and must be factored into COOP planning—as demonstrated by the 2006 theft of a Veterans' Administration-owned laptop that contained unencrypted social security numbers. Third-party security solutions provide:

- Secure transmission. Data exchanged between a smartphone another device can be protected in transit using Federal Information Processing Standards (FIPS) 140-2 encryption. Even if an outsider monitors cellular or WiFi transmissions, the e-mail content is unreadable.

- Secure storage. Government employees can encrypt the files on their smartphones to protect them from being viewed if the device is stolen. Employees or agencies can establish a policy to encrypt all stored files at specified intervals. Files can also be associated with a specific smartphone so that they become unreadable if synched to a laptop, for example, or if transmitted to another smartphone.
- Authentication. Equipped with the appropriate software and a Common Access Card (CAC)-card reader, smartphones support two-factor identification required to access protected databases.

Conclusion

The essence of COOP is enabling the business of government to continue, no matter what, in order to protect citizens' lives, crucial infrastructure, and the environment. COOP requires decentralization, resiliency, and flexibility. Smartphones play a vital role in COOP and emergency response by providing government employees with secure, flexible communications options in a single device. Employees can access the same information that they could from their office Internet connections: documents, spreadsheets, databases, images, and video. They can communicate securely within the agency or with other agencies via voice, e-mail, or text message. They can send multimedia messages quickly, to one person or many, by tapping the screen or speaking a simple voice command. Depending on what networks are available, government employees have multiple and redundant connectivity options, including the cellular network, WiFi, or satellite.

During disasters as well as everyday operations, a single low-cost device, the smartphone, helps agencies acquire communications resilience, improve decision-making with access to real-time databases, and enhance situational awareness to improve outcomes.

To read more about the use of Palm Treo smartphones in government, visit www.palm.com/government.

Palm, Inc.
950 W Maude Ave
Sunnyvale, CA 94085-2801
www.palm.com

P 523 06