A white paper by NEC Unified Solutions, Inc.

Government Continuity:

A Unified Disaster Response Providing Sustainable Communications and Interoperability

Empowered by Innovation

NEC

Executive Summary

Government continuity is the planning and management for sustaining services and communications by government entities during an emergency, event or incident. It allows a reaction to the situation and provides the necessary emergency response and recovery upon which constituents depend and expect.

According to the final report "A Failure of Initiative" by the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, "Better information would have been an optimal weapon against Katrina. Information sent to the right people at the right place at the right time. Information moved within agencies, across departments, and between jurisdictions of government, as well." Hurricane Katrina and a number of other major incidents have defined the challenges of providing consistent government services during a time of natural or manmade crisis.

The communications catastrophes of 9/11 and Hurricane Katrina made plain the importance of effective communications continuity planning and preparedness. Better information requires better telecommunications links, even in emergencies when all normal links are down.

This white paper outlines a disciplined three-step approach to planning and preparation that will substantially enhance continuity of government by planning for the simultaneous restoration and recovery. Government continuity supports uninterrupted social governance that can be measured through ongoing services. Continuity of these services can only be offered through a coordinated response involving sustainable communications and interoperability.

Problem/Opportunity

As America has evolved as a country and society, its citizens have become increasingly more dependent upon government. With this increasing dependency comes an equivalent increase in the American government's importance and responsibility. Today, a larger group of people rely on government, federal, state or local, for welfare and medical care, housing, retirement income, education and rural and agricultural services than ever before. This dependence upon the government is not limited to individuals either; businesses also rely heavily on government resources and daily operations. Government has permeated all levels and facets of life.

The Northeast Blackout of 2003, the largest blackout in North American history, affected an estimated 40 million people in eight U.S. states and 10 million people in Ontario and resulted in estimated financial losses between $4 billion and $10 billion. This event exposed weaknesses in communications and other critical infrastructure that detected unauthorized border crossings, port landings and access to vulnerable sites as well as emphasizing the ease with which power grids can be damaged. The blackout illustrates the lesson that restoration and provision of telecommunication services and electric power are critical for first responders and the restoration and recovery of all other critical infrastructures.

"Better information would have been an optimal weapon against Katrina."

"A Failure of Initiative"

The most obvious example is the series of coordinated suicide terrorist attacks on the United States on September 11, 2001, during which fire, police and Port Authority personnel experienced significant difficulties in communicating across service and jurisdictional boundaries. Accounting for and coordinating the responding units in New York City was difficult because of internal communications failures resulting from limited radio capabilities in the high-rise surroundings of the World Trade Center (WTC) and also from confusion over who was appointed to which frequencies. This confusion contributed to over-saturation of the radio channels. First responders lacked interoperability and unified command, both within and among the individual responding units. In their 2004 final report, the 9/11 Commission charged that "the task looking forward is to enable first responders in a coordinated manner with the greatest possible awareness of the situation." Central to this expectation of awareness is the ability to effectively and efficiently communicate across the entire disaster environment.

Both examples illustrate the communications essentials of government continuity: preservation of existing communications capability and provision of interoperability.

Preservation of Capability

During any incident deemed outside of normal operational parameters, government agencies must be able to communicate at the levels comparable to those experienced during times of normal operations. Government constituents largely have a "take it for granted" attitude about the routine services they receive from the public sector and an expectation that interruptions – if any – will be few and resolved quickly. Emotions can run high during a disaster situation, and people seeking normalcy look first to those services and activities that typically are always available.

In a 2006 survey conducted by the U.S. Conference of Mayors, the overall average response for how much the level of disaster preparedness has improved since 9/11 was 6.3 (on a scale of 1-10, 1 being the lowest and 10 the highest amount of improvement)[1]. While this number reflects progress, it shows there is still room for development and planning among local governments.

Interoperability

Interoperability for public safety communication is defined as the ability to share information via voice, data, on-demand, in real-time, when needed and as authorized.[2] The capacity for moving assets where needed most and sharing information allows governments and first responders to establish situational awareness and command and control operations, thereby managing constituents' fears and expectations during the emergency.

First responders must be able to coordinate their response with the greatest possible awareness of the situation to aid in mitigating the loss of lives and property. Therefore, interoperability must be included in government continuity planning.

Providing a Sense of Safety and Security

To provide constituents, businesses and other entities with a broad range of services and resources, federal, state and local governments rely heavily on communications – both interoperable and not – to secure and share information. When communication channels collapse or become unavailable, government operations are slowed or stop altogether, resulting in loss of monies, services, products and, in extreme cases, lives. Additionally, the inability to communicate puts citizens at a heightened level of vulnerability to criminal or even terrorist attack – a top of mind issue for many Americans today.

- 44% of cities report experiencing an incident in 2003 in which lack of interoperable communications made response difficult
- 49% of cities report not having interoperability with state police
- 60% of cities are not interoperable with their state emergency operations centers (EOC)
- 83% of cities are not interoperable with the Department of Justice
- 88% of cities are not interoperable with Homeland Security

U.S. Conference of Mayors Interoperability Survey [3]

What is Government Continuity?

Government continuity, as an extension of business continuity, consists of the advance planning and preparations by government – local, state and federal – for use during an emergency, event or incident that may result in interruptions of daily operations. It allows government to react to the situation and provides the necessary emergency response and recovery upon which constituents depend and expect.

Government continuity includes planning not just for flashlights, batteries and water, but also for backup communications in case of power failure or damaged infrastructures. It incorporates preparations for interoperability among first responders, EOCs and other government officials and operations.

Business Continuity – The Foreshadowing Of A Solution

During the 1990s, the private sector started developing business continuity as a concept and practice. Pressure from investors, regulatory agencies and resulting industry standards prompted an increase in planning and an evolution of business continuity into a well-recognized discipline.[4] However, operational continuity is not limited to the private sector. In actuality, it affects all levels of government, as shown by the above examples.

Clearly, the opportunity exists for many state and local governments to build on what business and industry have learned, creating a system to establish or enhance continuity planning and communications. There are two essential requirements that must be considered in government continuity planning: maintaining any communications capabilities remaining immediately after an incident and rapidly restoring communications capabilities on a prioritized basis.

Impact of Problem on Audience

If government entities are unable to maintain communications, doubt begins to develop among its constituents as to the government's competence in its other duties and tasks. Also, those entities are often unable to achieve the expected standards of performance during times of emergency, resulting in loss of lives, property or both.

- 18% of state officials report that emergency communications difficulties among federal, state and local authorities still exist
- 55% of cities report that issues with equipment and technology are obstacles to achieving interoperability
- Overall average age of communications systems in cities is 8.66 years old

Western Carolina University 2006 survey [5]
U.S. Conference of Mayors Interoperability survey [6]

One of the greatest and most recent examples of a communications failure during an emergency was witnessed during Hurricane Katrina. More than three million customer telephone lines were destroyed in Louisiana, Mississippi and Alabama. Thirty-eight 911 call centers were inoperative, and two telephone company switches in New Orleans in charge of routing 911 calls for neighboring parishes were eliminated by the flooding, resulting in a significant loss of capacity in and around New Orleans. Although the equipment and knowledge that allows 911 calls to be switched to an alternative location is available, many of the Louisiana 911 call centers did not have the procedures prepared to identify where calls should go and had not coordinated for any rerouting. As a result, many 911 calls were dropped in the direct after-effects of the storm.[7]

"Communications and coordination was lacking, preplanning was lacking. We were not prepared for this," according to William M. Lokey, FEMA Federal Coordinating Officer in Louisiana, testimony before U.S. Senate, Jan. 30, 2006.

Given the broad extent of damage, preservation of basic services was understood to be unavailable in the period immediately following the hurricane. However, interoperability was the biggest communications challenge and concerns in government response to Katrina – whether communications facilities failed, destroyed or were incompatible. For instance, hundreds of New Orleans first responders tried to communicate on only two radio channels, creating communications gridlock to transmit or receive information as they waited for an available channel on which to communicate. Louisiana's state EOC had such serious communications problems that state officials could not share information with local officials, others in the state government or federal officials, emphasizing the already critical problems with situational awareness.

"It sounds like it can happen again. How many local governments have a communications plan when everything fails?" asked Representative Tammy Baldwin (D-WI), during a U.S. House of Representatives hearing on Sept. 7, 2005.

Dependable and consistent communications are critical to the preparation for and response to any catastrophic event because of the influence it has on establishing command and control and maintaining situational awareness. Constituents also rely on reliable communications because without the ability to call for help, they cannot seek emergency assistance, alert responders or others to their whereabouts and needs, or receive updates or instructions from officials.

A Three-Step Approach

"Technology is at the center of this, but most of the components required to achieve interoperability in the near-term already exist. However, it requires agreements, planning, and governance arrangements across jurisdictions," stated David Boyd, Deputy Director, Office Systems Engineering & Development, in a DHS Testimony before U.S. Senate on Sept. 29, 2005.

Government continuity must support uninterrupted social governance that can be measured through the services provided. Continuity of these service offerings can only be offered through a coordinated response involving sustainable communications and interoperability.

> **"(Interoperability) requires agreements, planning, and governance arrangements across jurisdictions."**
>
> David Boyd, testimony before U.S. Senate

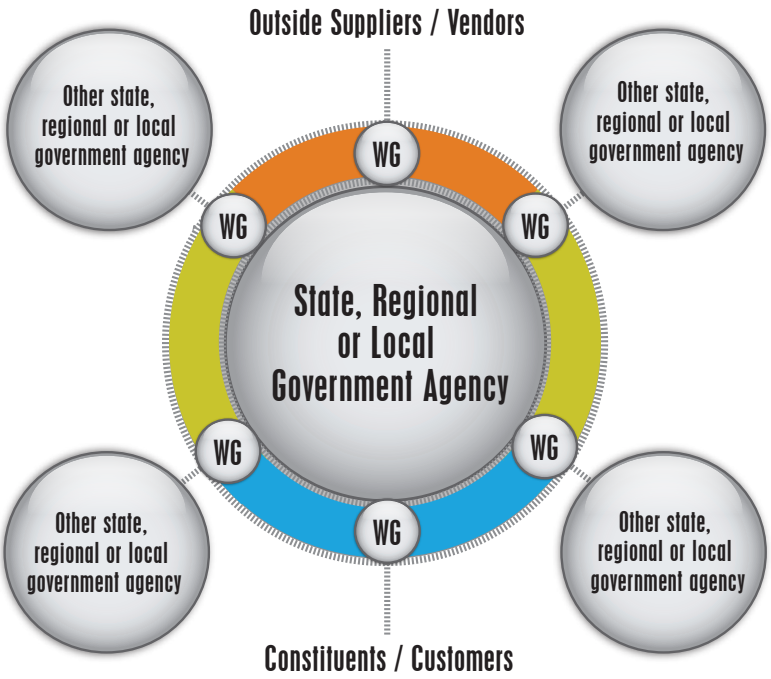
Disasters are not limited in responsibility to the federal government. After the federal government has withdrawn from the immediate situation, state and local government continue to manage recovery and restoration. Therefore, state and local officials need to make responsible use of available federal, state and local funding to develop communications systems that can and be in place in the event of a disaster.

There are three major stages in continuity planning to consider when creating an effective government continuity plan: (1) assessment and prior planning, (2) inventory of current tools and capacity, and (3) rationalization and change in procedure and assets.

Assessment and Prior Planning

In the assessment and prior planning stage, the first step is to determine the desired state of readiness, as well as the specific agency responsibilities and communications deliverables, to be delivered both on a routine basis and during a state of emergency.

Second is to identify all groups with whom the agency must communicate, routinely and in the event of an incident. These might include citizens, outside suppliers/vendors and other state, regional or local government entities who contribute to or benefit from agency operations (Figure 1).



WG = Work Group
Figure 1 – Diagram of communication with audiences for government agency

Third is to determine what communications tools and channels are required to establish and maintain open communication with all three major target audience categories, on both a routine basis and during a state of emergency (Figure 2). It is important to note that while communication tools may be traditionally self-supporting, this planning exercise affords an opportunity to increase integration of various tools into a single, unified communications system. It takes the efforts of each approach for communications to remain operational and effective during a crisis. A more unified communications environment increases messaging efficiency, requiring fewer resources to communicate effectively.

Finally, priorities for communication restoration must be established, i.e. what teams and individuals absolutely need to be able to communicate during the earliest stages of an emergency.

	Local agency	Supplier/ vendor 1	Supplier/ vendor 2	Supplier/ vendor N	Other gov agency 1	Other gov agency 2	Other gov agency N	Citizens
Telephone	X	X	X	X		X	X	X
E-mail	X	X	X	X	X	X	X	X
Fax		X	X	X	X		X	
Mail		X		X				X
Two-way Radios	X				X	X	X	
Mobile Phones	X				X	X	X	
Digital Signage								X
Pagers	X				X		X	
Satellite Phones/ Radios					X		X	
Sms Text			X	X				X
Internet			X	X				X

Figure 2 – Map of audiences (using Figure 1) and communications tools

Early in the planning process, it is essential to understand how communications associated with both routine and incident-oriented events are similar and how they are different. In order to facilitate communications, plans must categorically take into account the groups and individuals with whom the agency needs to communicate, and how each is prioritized in the overall plan. Part of this identification process should include determination of interoperability requirements across departments or jurisdictions. In some instances, absolute interoperability may be a requirement. However, in others, gatekeeping between different agencies or between departments within a single agency may be important to ensure movement and handling of priority activities can occur.

Inventory

Equipped with documented routine and incident communications needs, agency leadership needs to inventory existing communication systems under both situations. Planners should list and evaluate the communications tools and capacities needed, including the number of platforms and type of equipment – those that are interoperable and that are not – across the key constituents or audiences identified. This will illustrate which channels and equipment are available, the working status of each, what needs to be updated and what gaps in tools used to meet current operational and anticipated incident communications to address.

Resources applied in government continuity planning to maintain operations and communications during disasters include:

- Telephones (number, location, capacity and nature of connectivity – traditional circuit-switched, Voice over IP, microwave, cellular and/or satellite)
- Radio equipment – handheld, portable, mobile, fixed
- Radio bandwidth – licensed frequencies
- Other personal communications devices – voice and display paging, connected PDAs and multi-function, RF-based devices
- Geographic Information Systems
- Display apparatus – large-scale signage
- Servers, printers, scanning devices cameras and other voice, video and data peripherals
- Internal and external networking (LAN, WAN, Intranet, Extranet, Internet), both primary, and secondary or back-up
- Backup generators and fuel
- People with expertise

Beyond physical assets, the inventorying stage should also include technical expertise in voice, video, data, telephony, mobile radio, RF, LAN/WAN/TCP-IP and other disciplines deemed pertinent to an agency. Their knowledge of prospective membership in an issues or crisis team and knowing how to reach each using multiple communications channels or methods are essential considerations often overlooked in continuity planning.

Rationalization and change

In the rationalization and change stage, information gathered and identified should be evaluated with an eye toward necessary modifications in agency approach and preparedness for non-routine communications. The primary goal of this stage is to define and implement steps required to shrink and, ultimately, eliminate the gap between current and desired levels of preparation and survivability.

After the change stage has been completed, evaluation of the plan should occur to measure current preparedness. At a time in the reasonable future, the plan should be reevaluated to integrate any changes in personnel, operations and/or resources. If it is determined that updating the plan is required, beginning again at stage one will increase the levels of preparedness and survivability.

"The goal of developing a plan for government continuity is to reduce the seriousness and extent of any unmitigated situations that may arise during various types of incidents."

Doug Martinez, Director of Government Accounts, NEC Unified Solutions

In creating an effective government continuity plan, the following should be considered:

- Identify the means of communication that can reasonably be expected to be available in a range of predictable situations; what capabilities and limitations may exist under projected incident situations
- Determine how each type of communications systems likely will respond to overload and damage, through an appropriate combination of drill and modeling activities; this response information will contribute to decisions that will be made during an emergency as to what systems to use, and when and what forms of backup likely will need to be called into service
- Include a point of view regarding use of multiple or redundant communications modes, basing the decision on a balance of risk and impact assessment, because no single system is the universal answer or any more stable and secure than another; identify those systems for which no practical source of redundancy is available and have in place a contingency plan for minimizing the impact of such systems' loss
- Ensure that all personnel – both those implementing incident-based communications and those using such systems – are familiar with and have access to alternative communications equipment and channels that will come into use for maintenance of government continuity in any form of communications emergency

In creating a change model to prepare for non-standard operations, it is important to convey that the purpose of all planning and preparation for government continuity is aimed at significantly reducing uncertainty in a time of emergency, but that no degree of planning can completely eliminate this anxiety. The goal of developing a plan for government continuity is to reduce the seriousness and extent of any unmitigated situations that may arise during various types of incidents that reasonably can be anticipated and for which planning can occur.

[1] "Five Years Post 9/11 and One Year Post Hurricane Katrina: The State of America's Readiness." The U.S. Conference of Mayors. Released July 26, 2006.
[2] "A Failure of Initiative: The Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina." The Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. Released February 15, 2006.
[3] "The United States Conference of Mayors Interoperability Survey." The U.S. Conference of Mayors. Released June 27, 2004.
[4] "The History of Business Continuity: A Timeline." http://www.businessresiliency.com/evolution_history.htm
[5] "National Survey of State Homeland Security Officials." Institute for the Economy and the Future. Western Carolina University: Released May 2006.
[6] "The United States Conference of Mayors Interoperability Survey."
[7] "A Failure of Initiative."

About NEC Unified Solutions, Inc. NEC Unified Solutions Inc., a global leader in VoIP and data communications for the enterprise and small-medium business, delivers the industry's most innovative suite of products, applications and services that help customers achieve business value through technology. NEC Unified Solutions, a wholly owned subsidiary of NEC Corporation of America, offers a complete portfolio of solutions for wireless, unified communications, voice, data and management services, and an open migration path to protect investments. NEC Unified Solutions, Inc. serves Fortune 1000 customers across the globe in vertical markets such as hospitality, education, government and healthcare.

For more information, visit www.necunified.com

NEC
Empowered by Innovation