Continuity of Operations Planning and E-Government

R. Eric Petersen
Congressional Research Service, USA

Jeffrey W. Seifert
Congressional Research Service, USA

INTRODUCTION

Continuity of operations (COOP) planning, sometimes referred to as disaster recovery planning, business continuity planning, or business resumption planning, is a segment of contingency planning that refers to the internal effort of an organization, such as a branch of government, department, agency, or office, to assure that the capability exists to continue essential operations in response to a comprehensive array of potential operational interruptions. In government, COOP planning is critical because much of the response to an incident might include the maintenance of civil authority and infrastructure repair, among other potential recovery activities. All such efforts presume the existence of an ongoing, functional government to mobilize, fund, support, and oversee recovery efforts. In an emergency, government is likely to need to ensure the ability to communicate with internal and external constituencies. This function is becoming associated with electronic government. For example, many people in the United States and elsewhere, when searching for information and guidance following the September 11, 2001 attacks, turned to government agency Web sites. Beyond such extraordinary examples, the growing public expectations of e-government has put additional pressure on the need to reconstitute systems quickly after an interruption to minimize any disruptions and financial costs associated with a major infrastructure failure.

Government COOP planning may be regarded as a "good business practice," and part of the fundamental mission of agencies as responsible and reliable public institutions. Comprehensive contingency plans, perhaps once viewed, at the least, as optional and, at the most, as a prudent measure, are now seen as an integral part of developing and maintaining an agency's capacity to carry out its essential functions. Continuity planning professionals assert that the perception of a changing threat environment and the potential for no-notice emergencies, including localized acts of nature, accidents, technological emergencies, and military or terrorist attack-related incidents, have increased the need for COOP capabilities and plans that enable agencies to continue their essential functions across a broad range of potential emergencies. COOP planning can be viewed as a continuation of basic emergency preparedness planning, including evacuation planning, and serves as a bridge between that planning and efforts to maintain continuity of government in the event of a significant disruption to government activity or institutions. In the aftermath of an incident, initial efforts typically focus on safeguarding personnel and securing the incident scene. Subsequently, attention focuses on reestablishing critical agency operations according to a COOP plan. Because the number and types of potential interruptions are essentially infinite, effective COOP planning must provide, in advance of an incident, a variety of means to assure contingent operations.

In the context of e-government, the heavy reliance upon information technology to carry out mission critical tasks and provide other citizen services highlights the need to ensure these assets are robust, protected, backed up, and resilient to interruption. COOP is not a new idea. While contingency planning has gained considerable attention in recent years due to heightened security concerns and increased dependence on information technology, modern government continuity planning has been practiced, in one form or another, for several decades. What may now be emerging is a recognition that all organizational assets, in the case of government, this would include leaders, civil servants, and information infrastructures, must be incorporated into organization-wide contingency planning.

EVOLUTION OF GOVERNMENT CONTINGENCY PLANNING

Government contingency planning grows out of two major streams. One stream, COOP planning, focuses generally on the preservation of staff, facilities, technology systems, and data. The other stream, sometimes identified

as continuity of government (COG), typically focuses on preserving government leadership and high-level officials. Depending on the scope of an operational interruption, COOP and COG plans could be initiated independently or in concert with one another. The failure of the network supporting a regional or national e-government program could be a COOP event. The failure of such a system as a result of war or terror attack on government facilities could also be a COG event if critical national functions are interrupted, or leaders are the target of the incursion. Due to the wide variety of potential operational interruptions, it is all but impossible to make a firm delineation between COOP and COG activities used to support e-government programs that could be generalized across all nations. As a consequence of security concerns, current government contingency plans, whether they are those that focus on localized or low level operational interruptions, or those that threaten the safety and welfare of state leaders, are not public information, and are not widely available within government. The history of government contingency planning strongly suggests, however, that it is reasonable to assume that contingency planning for government leaders, their staffs, and the facilities that support government operations are closely interrelated.

Leadership preservation is the more longstanding contingency practice. For example, Tanfield (1991) found that, before World War II, there was a confidential plan for the evacuation of the United Kingdom's Parliament from Westminster to a secret location (later revealed as Stratford-Upon-Avon) prior to the commencement of hostilities, although this plan was never used. During the war, Parliament was forced to convene outside of its traditional setting after the chambers of the House of Commons were destroyed during an air raid. For the remainder of the war years there was a ban on disclosing the location of Parliament. Similarly, the governments of The Netherlands and France continued to operate from abroad while their nations were occupied.

In the United States, Cold War efforts to preserve leaders and institutions of government focused on preserving the continuity of government in the event of a nuclear conflict with the former Soviet Union. Federal contingency planning focused on preserving the line of presidential succession, by safeguarding officials who would succeed the president. Also, Cold War era plans reportedly included locating and evacuating the officials in the line of succession, along with the other senior leaders of cabinet departments, as well as members of the U.S. Congress and justices of the Supreme Court. In the event of an imminent nuclear attack, the plans called for the relocation of these individuals to secure, alternative operational facilities outside of Washington, DC (Blair, Pike & Schwartz, 1998; Gup, 1992a, b; Zuckerman, 1984).

As leadership-focused plans evolved, it was recognized by emergency planners that it could be necessary to support the country's senior leadership, or to carry out critical functions in the aftermath of an attack, regardless of the need to evacuate and relocate government officials. Consequently, COOP planning became a unifying element that integrated support functions in situations where the lack of such basic support components as personnel, alternative operational facilities, information technology assets, or records posed the potential threat of serious disruption to operations and the ability of the government to provide services and carry out its duties.

In the period following the end of the Cold War, and reinforced by experiences surrounding the September 11, 2001 attacks in the United States, the March 11, 2003 train bombings in Spain, the July 7, 2005 attacks on the London Underground, and attacks on diplomatic and commercial facilities around the world in the past ten years, contingency planning has evolved. Once considered as remote possibilities, the permanent loss of a facility, or the impairment of staff due to radiological or biological contamination, while still unlikely, are now taken more seriously. Recently, for example Cracknell and Elliott (2005) reported that the United Kingdom Parliament, which has not been denied the ability to use its primary facilities since 1681, exercised its plan to relocate Members of Parliament from the Palace of Westminster to another facility approximately 50 miles away from central London. Nevertheless, contingency planners have recognized that contingency plans based on Cold War era assumptions that included a period of warning before an attack, are inadequate protection in a threat environment characterized by potential sudden, localized terrorist attacks by non-state actors that could include the use of weapons of mass destruction (Bhambhani, 2001; Milbank, 2001; Pressley & Hsu, 2003). Accordingly, attention to contingency planning has extended to and incorporated planning to protect vital information technology (IT) assets.

As with the stream of planning that focuses on preserving leaders and staff, government (COG) IT disaster recovery planning has evolved with advances in technology, equipment, and information resources over the past 25 years. At various times, disaster recovery planning preparations have been incorporated into infrastructure and software upgrades deployed in response to emerging events, such as Year 2000 (Y2K) planning, the successive waves of computer virus and worm incursions, and physical attacks on people, buildings, and infrastructures.

While much of the current attention to COOP planning focuses on responding to potential attacks, operational interruptions that are more likely to occur and could necessitate the activation of a COOP plan include routine building renovation or maintenance; mechanical failure of heating or other building systems; fire; and inclement