Order Code RL31594

Report for Congress
Received through the CRS Web

Congressional Continuity of Operations (COOP): An Overview of Concepts and Challenges

Updated January 14, 2003

R. Eric Petersen
Analyst in American National Government
Government and Finance Division

Jeffrey W. Seifert
Analyst in Information Science and Technology Policy
Resources, Science, and Industry Division

Congressional Continuity of Operations (COOP): An Overview of Concepts and Challenges

Summary

Interruptions of congressional operations by incidents such as episodic computer virus infections, or the anthrax contamination that took place during autumn 2001, have demonstrated the importance of congressional continuity of operations (COOP) planning. COOP planning refers to the internal effort of an organization to assure that the capability exists to continue essential functions in response to a comprehensive array of potential operational interruptions. For Congress, COOP planning is related to a second level of preparedness, continuity of government (COG) planning. Congressional COG planning focuses on ensuring that Congress is able to carry out its legislative responsibilities under Article I of the Constitution.

This report discusses the circumstances surrounding COOP planning, including provisions for alternative meeting sites and methods for conducting House and Senate meetings and floor sessions when Capitol facilities are not available. Although this report does not discuss COG planning beyond its direct relationship to COOP planning, a more comprehensive analysis of COG can be found in CRS Report RS21089, *Continuity of Government: Current Federal Arrangements and the Future*.

The task of ensuring that Congress can continue to carry out its constitutional responsibilities in case of disruption, presents unique challenges in addition to the operational concerns common to most organizations. One challenge involves the relocation of legislative activities. There appears to be no constitutional bar to the House and Senate adopting a resolution that approves meetings of either chamber outside the Capitol in advance of doing so. In addition, the rules of each chamber allow for committee activity beyond Washington, DC. However, concerns regarding the availability of appropriate alternative facilities, communication and technical capabilities, and providing the necessary physical security, have arisen.

Other concerns regarding physical security have prompted some observers to propose creating a virtual or electronic Congress (e-Congress). Although these suggestions have generally focused on the creation of a Web site accessible by Members anywhere in the country, it is unclear exactly how an e-Congress would be constituted and operated. Other challenges for COOP planning include maintaining Member office information security, and the Legislative Information System (LIS).

Although current congressional COOP planning began prior to September 11, 2001, details surrounding House and Senate COOP planning are not publicly available, and some specific information is excluded from this report to preserve operational security. Contingency planning in the House, however, has evolved over the past 20 years and there exists a range of backup strategies for maintaining critical House legislative and administrative information systems. In the Senate, initial COOP planning was completed in spring 2002, and continues to be refined.

Contents

Introduction 1

Recent Activities and Challenges 3
COOP Planning Prior to September 11 3
Impact of September 11 and Anthrax Incidents 4
House COOP Planning 6
Senate COOP Planning 7

Current Issues and Proposals 9
Relocating Legislative Activities 9
Floor activity 9
Committees 10
Electronic Sessions and Legislation in the 107th Congress 11
Member Office Information Security 12

Additional Considerations 13

Selected Glossary of COOP-Related Terms 13

Additional Reading 16

Congressional Continuity of Operations (COOP): An Overview of Concepts and Challenges

Introduction

The autumn 2001 terrorist attacks on the United States, and increasing dependence of organizational functions on advanced information technology (IT), have brought renewed attention to the need for organizations to engage in continuity of operations (COOP) planning. Recent interruptions of congressional operations through both computer virus infections[1] and terrorist attacks have demonstrated that these concerns and needs extend to Congress, as well as to other private and public institutions. Some private sector activities can be relocated or reconfigured to respond to continuity threats by dispersing centralized facilities, installing automated backup systems, or maintaining excess capacity. The task of ensuring that the 540 Members of Congress can continue to carry out their constitutional responsibilities in case of disruption presents special and unique challenges in addition to the operational concerns common to most organizations. An attack against Congress could result in a loss of individuals critical to governance, destroy important symbols of government, and undermine the national sense of safety and security.

Continuity of operations planning refers to the internal effort of an organization, such as an office or department, to assure that the capability exists to continue essential functions in response to a comprehensive array of potential operational interruptions. COOP planning is an *ongoing process* that is driven in part by growth and change of information systems, personnel, and mission critical needs. Operational interruptions may include routine building renovation or maintenance; mechanical failure of heating or other building systems; fire; inclement weather or other acts of nature; or a range of threatened or actual attacks. Other events which may interrupt congressional activity include failure of information technology (IT) and telecommunications installations due to malfunction or cyber attack.[2] For Congress, these interruptions might affect an individual office, building, or the entire Capitol complex. As the anthrax incidents in the Hart Senate Office Building

---

[1]Ian Hopper, "Destructive 'ILOVEYOU' Computer Virus Strikes Worldwide," *CNN.com*, May 4, 2000, [http://www.cnn.com/2000/TECH/computing/05/04/iloveyou/].

[2]A cyber attack is an incursion on a range of IT facilities, and can range from simply penetrating a system and examining it for the challenge, thrill, or interest, to entering a system for revenge, to steal information, cause embarrassment, extort money, cause deliberate localized harm to computers, or damage to a much larger infrastructure, such as telecommunications facilities. See CRS Report RL30735, *Cyberwarfare*, by Steven A. Hildreth.

demonstrated, recovery from these incursions may not be immediate, and may require the relocation of Members of Congress and congressional staff, infrastructure, and operations for prolonged periods of time.

For Congress, COOP planning is related to a second level of preparedness, continuity of government (COG) planning. COG planning involves the ability of an entire branch of government to carry out its functions. Congressional continuity of government planning focuses on ensuring that Congress is able to carry out its legislative responsibilities under Article I of the Constitution. In Congress, this can include preserving the line of succession to the presidency, as well as establishing an alternative meeting site for Congress.[3] A third level of preparedness, enduring constitutional government (ECG), which is not addressed in this report, involves planning by the legislative, executive and judicial branches of government to maintain the ability to assure the survival of the country's constitutional, representative form of government in the event of a catastrophic emergency.

COOP and COG plans can be activated independently. Under most circumstances a COOP plan could be activated when there is no COG threat. However, many believe that to ensure the ability of the legislative branch to provide essential services to citizens and carry out critical functions, integration of the two types of planning is necessary to ensure the efforts developed under each plan will work together seamlessly when necessary.

This report discusses the circumstances surrounding congressional continuity of operations planning. It also discusses the backup, maintenance, and portability of various administrative functions used to support Congress, such as legislative information, e-mail, and the continuity of congressional information technology (IT) and enterprise systems.[4] Plans and details surrounding COOP planning are not publicly available, and some specific information is excluded from this report to preserve operational security. A glossary of COOP planning terms is included in the appendix. This report does not discuss COG planning beyond its direct relationship to COOP planning. For a more comprehensive analysis of COG, see CRS Report RS21089, *Continuity of Government: Current Federal Arrangements and the Future*.

---

[3]Under the Presidential Succession Act (61 Stat. 380; 3 U.S.C. 19), the line of presidential succession passes to the Speaker of the House and President pro tempore of the Senate, if the President and Vice President are unable to carry out their duties. Continuity of government planning provides mechanisms to preserve the line of succession, but is not considered in this report. See CRS Report 98-731, *Presidential and Vice Presidential Succession*, by Thomas H. Neale, and CRS Report RS21089, *Continuity of Government: Current Federal Arrangements and the Future*, by Harold C. Relyea. See CRS Report RS21068, *House Vacancies: Selected Proposals to Allow for Filling Them Due to National Emergencies*, by Sula P. Richardson, for a detailed analysis of recent proposals to fill vacancies in the House of Representatives.

[4]Enterprise is often used in the computer industry to describe any large organizations, including corporations, small businesses, nonprofit institutions, or government bodies, that utilize computers. In practice, the term is applied much more often to larger organizations than smaller ones. An intranet, an internal system of sharing data and software, is an example of an enterprise computing system.

Recent Activities and Challenges

Most, if not all, government institutions have had plans to restore operations or continue operations in the face of an emergency. During the Cold War, Congress itself established a secret, remote meeting site several hours removed from Washington, DC, where it might reconvene and resume its constitutional responsibilities in the event of a nuclear attack. Also, over the last 20 years, Congress has worked to incorporate disaster recovery planning into its infrastructure and software upgrades.

COOP Planning Prior to September 11

Current congressional COOP planning began pursuant to a joint bipartisan leadership directive[5] issued on September 6, 2000, directing the Capitol Police Board[6] to "develop and manage" a "comprehensive Legislative Branch emergency preparedness plan." To facilitate this effort, the board was to work "with the Attending Physician and the Chief, US Capitol Police, and in coordination with the Officers of the Senate and House" to develop "an integrated architecture which will address all hazards which could impede the continuity of essential Legislative Branch functions." According to the directive, this integrated architecture is to include "at a minimum, emergency preparations, response, mitigation and stabilization activities, and recovery operations."

Congressional COOP planning has been developed from the bottom up, beginning with the identification of critical operational infrastructure and resources, and creating plans to maintain those capabilities in the event of a wide range of unforseen circumstances. Individual COOP plans are activated by specific events that interrupt routine congressional operations, and focus on restarting those operations. The explicit goal of COOP planning is to ensure that congressional operations can be performed under any circumstances. The activation of a COOP plan by one or more offices in Congress is law enforcement sensitive, and is based on ongoing threat level assessment and the discretion of relevant officials. Because there is more than one way to interrupt congressional activity, both House and Senate planners are developing a variety of contingency plans to respond to a range of potential operational interruptions. By design, COOP plans are meant to be living documents, revised regularly on the basis of emerging issues and needs assessments. A component of this revision process includes congressional staff education and training to execute their responsibilities under their COOP plans.

---

[5]Trent Lott, Senate Majority Leader, J. Dennis Hastert, Speaker of the House, Thomas A. Daschle, Senate Minority Leader, Richard A. Gephardt, House Minority Leader. September 6, 2000. "Directive to the United States Capitol Police Board."

[6]The Capitol Police Board is comprised of the Sergeants at Arms of the House and Senate and the Architect of the Capitol.

Impact of September 11 and Anthrax Incidents

Comprehensive COOP planning was already underway when, in the fall of 2001, terrorists attacked the World Trade Center and the Pentagon, and later several congressional office buildings were closed due to anthrax contamination. Those events added a sense of urgency to the planning process begun a year earlier.

On September 11, 2001, following reports of the Capitol being a potential next target, some units of the Senate officers' staffs activated their COOP plans, and COG plans were activated in the House and Senate. The leadership of both chambers was moved to an undisclosed, secure location for briefings.[7] Despite the evacuation of all congressional buildings, including the Capitol, congressional offices, and the Library of Congress, the events of September 11 did not cause any lasting interruption of essential congressional operations. In some cases, Members and staff were able to return to their offices and resume activity later in the day, and both chambers were back in session on September 12.[8]

In October 2001, concerns regarding anthrax contamination of congressional buildings resulted in the closure of offices, and the postponement of hearings in both the Senate and the House of Representatives, as well as a temporary recess of the House of Representatives. On Monday, October 15, an anthrax-contaminated letter was opened in Senator Thomas Daschle's office, exposing more than two dozen people to the bacteria. The following day, the southeast corner of the Hart Senate Office building, including the offices of 12 Senators, was closed to limit further exposure and spread of the powdery substance. On Wednesday, October 17, Speaker Dennis Hastert announced a 5-day recess while House buildings were tested for anthrax contamination. Also that day, Senate Majority Leader Daschle announced the closure of all Senate office buildings to facilitate testing, but the Senate remained in session as originally scheduled.

On Monday, October 22, the Capitol building was reopened, and both the House and the Senate returned to session on Tuesday, October 23. On October 24, the Russell Senate Office Building was reopened, followed by the reopening of the Cannon and Rayburn House Office Buildings on October 25. The Dirksen Senate Office Building was reopened on Friday, October 26. On Monday, November 5, the Longworth House Office Building was reopened, with the exception of three Member offices where trace amounts of anthrax were detected. These offices remained closed while environmental remediation to remove the anthrax spores took place.[9] Portions

---

[7]John Lancaster and Helen Dewar, "Outraged Lawmakers Vow to Keep Hill Going; Briefly Evacuated, Congress Returns To Show Resolve," *The Washington Post*, Sept. 12, 2001, p. A21; and Lauren W. Whittington and Mark Preston, "Sorrow and Defiance: Security Review Planned," *Roll Call*, Sept. 13, 2001, p. 1.

[8]"Issues Over Funds Control Stalls $40 Billion Bill," *CNN.com*, Sept. 14, 2001, [http://www.cnn.com/2001/US/09/13/congress.terrorism/].

[9]Michael Gerber, "Anthrax Found in Kennedy, Dodd Offices," *The Hill*, Nov. 21, 2001, [http://www.hillnews.com/112101/anthrax.shtm]; "U.S. House Offices to Reopen After Anthrax Scare," *Reuters*, Nov. 5, 2001, [http://sg.tech.yahoo.com/reuters/asia-70270.html].

of the Ford House Office Building were reopened on Tuesday, November 6.[10] Offices on the south side of the first floor of the Ford House Office Building, which had remained closed for environmental remediation, were reopened on January 22, 2002. The basement mail room of the Ford House Office Building has been remediated but not reoccupied.[11] The Hart Senate Office Building, which houses 50 Member offices, remained closed from October 17, 2001 to January 22, 2002.[12]

The Russell and Dirksen Senate Office Buildings were briefly closed again on Saturday, November 17, following the discovery of an anthrax-laced letter addressed to Senator Patrick Leahy. Although the Leahy letter was recovered from one of the 280 barrels of congressional mail being held and examined by the Federal Bureau of Investigation (FBI), officials were unsure where in the delivery process the letter had been intercepted. The two Senate office buildings were reopened Monday, November 19.[13]

In addition, many Members of Congress and staff had to relocate to alternate facilities while House office buildings were closed. The General Accounting Office (GAO) provided work facilities, equipment, and supplies for all 440 House Members and two staffers per Member of Congress, as well as for more than 20 House committees.[14] Preliminary COOP plans were activated when House officers prepared a temporary alternate facility for floor operations at Fort McNair in the southwest quadrant of Washington, DC. However, the plan was not implemented due to the reopening of the Capitol.[15]

Some Senators with Capitol offices worked out of them. Other Senators moved their office operations to nearby townhouses, apartments, state offices, or even cars parked in front of the Capitol.[16] Some Senators with offices in the Russell and

---

[10]Michael Gerber, "Anthrax Found in Kennedy, Dodd Offices," *The Hill*, Nov. 21, 2001, [http://www.hillnews.com/112101/anthrax.shtm]; Guy Taylor, "District Sees Threat of Anthrax Waning," *Washington Times*, Nov. 7, 2001, p. A3.

[11]See the House Advisory Information Page for the most recent information regarding the status of House buildings [http://www.house.gov/].

[12]Helen Dewar, "Senate Reclaims Russell Bldg.; Section of Hart Tests Positive," *The Washington Post*, Oct. 25, 2001, p. A29.; "Hart Fumigation Appears Successful," *The Washington Post*, Jan. 2, 2002, p. A2; Spencer S. Hsu, "Hart Reopening Delayed After Discovery in Ceiling," *The Washington Post*, January 18, 2001, A1; Spencer S. Hsu, "'It's Good to Be Back': Senators Return to Hart; Offices Reopen After 96-Day Anthrax Quarantine," *The Washington Post*, Jan. 23, 2002, p. A1.

[13]Michael Gerber, "Anthrax Found in Kennedy, Dodd Offices," *The Hill*, Nov. 21, 2001, p. 1, and [http://www.hillnews.com/112101/anthrax.shtm].

[14]Tanya N. Ballard, "In Anthrax Aftermath, GAO Turns to Telecommuting," *Government Executive Magazine*, Nov. 1, 2001,
[http://www.govexec.com/dailyfed/1101/110011t1.htm].

[15]Susan Crabtree, "Ft. McNair Ready for House Action," *Roll Call*, Nov. 1, 2001, p.1.

[16]William Matthews, "E-Mail Keeps Lawmakers in Touch," *Federal Computer Week*, Oct. 29, 2001, p. 12; Betsy Rothstein, "Anthrax Crisis Makes Members Displaced Persons," *The*
(continued...)

Dirksen buildings offered to share space with colleagues locked out of the Hart building.[17] In addition, Senate staffers were relocated to first aid stations, mail rooms, and the offices of the Senate Chaplain, as well as space in the Postal Square facility.[18] Some staff worked from home, or moved to nearby state offices as well.

Although alternate office accommodations were in place, office computer and hard copy files in the closed offices were, in many cases, at least temporarily inaccessible. Members of Congress and their staff adapted quickly to a changing environment and improvised to ensure that the business of Congress continued. However, the extended nature of the problems with the Hart Senate Office Building, and the disruptions of mail delivery,[19] highlighted the necessity of ongoing contingency planning in the event of a larger scale incident involving congressional facilities.

House COOP Planning[20]

In the House of Representatives, contingency planning is far from a new concept. Disaster recovery planning by House Information Resources (HIR) has evolved with advances in technology, equipment, and information resources over the last 20 years. At various times, disaster recovery planning has been incorporated into infrastructure and software upgrades deployed in response to emerging events, such as Year 2000 (Y2K) planning, a series of computer virus incursions, and the September 11 attacks.

At present, there is a range of backup strategies for maintaining critical House legislative and administrative information systems maintained by HIR. These include workflow and enterprise systems, personnel and payroll operations, House Web site content, and the House legislative information management system (LIMS).[21] Responsibility for securing and backing up committee and Member hard

---

[16](...continued)
Hill, Oct. 31, 2001, [http://www.hillnews.com/103101/displaced.htm].

[17]Helen Dewar, "Senate Reclaims Russell Bldg.; Section of Hart Tests Positive," *The Washington Post*, Oct. 25, 2001, p. A29.

[18]Peter Nicholas, "Anthrax Closures Squeeze the Senate," *The Philadelphia Inquirer*, November 20, 2001, p. A01; Lauren W. Whittington and Mark Preston, "EPA Hedges on Hart," *Roll Call*, Nov. 29, 2001, p. 1.

[19]Mail delivery throughout Capitol Hill immediately ceased following the discovery of the anthrax-laced letter in Senator Daschle's office. The distribution of surface mail to Congress, which is now irradiated before delivery, resumed in late Nov. However, the irradiation process can delay delivery by approximately one week. Jason Miller, "With Mail Safety Still Iffy, Hill Upgrades E-mail," *Government Computer News*, Jan. 7, 2002, p. 14; Nick Anderson, "Congress Will Get Mail Again," *Los Angeles Times*, Nov. 28, 2001, [http://www.latimes.com/news/nationworld/nation/la-112801mail.story].

[20]This section is based on discussion with staff in House Information Resources (HIR), and other sources, as noted.

[21]The House legislative information management system contains the metadata(or data about
(continued...)

copy office information and computer data, including e-mail and office Web sites, resides in each office. Among information technology professionals, the need for contingency planning for the preservation of enterprise information is an industry standard. In Member and committee offices, the sensitive nature of the information suggests that data backup and recovery strategies will need to strike a balance between control of the information and its relationship to a comprehensive House-wide data recovery plan.

In other matters of COOP planning, the House of Representatives continues to consider options for relocating floor activities in the event that Capitol facilities are unavailable. Member communications have been upgraded, with the Committee on House Administration issuing a BlackBerry, a wireless personal digital assistant, to each Representative. The purpose of the device is to communicate critical information to Members when other modes of communication may be inoperative.[22]

Other COOP issues, including planning for the relocation of House committee and Member office activities, as well as the development of enhanced capabilities offered by secure offsite backup and retrieval of critical data, are under consideration by House officers.

Senate COOP Planning[23]

In response to the joint bipartisan leadership directive, and guidance from the Senate Sergeant at Arms, the Senate's initial COOP plan was completed in the spring of 2001, with implementation of the plan constituted in three phases. The first phase involved the relocation of the Senate chamber and support staff needed to carry out floor business. The second phase focused on maintaining the operations of Senate officers, including the operational and technical infrastructure of the Secretary of the Senate and Sergeant at Arms. The final phase involved ensuring the continued operation of Member and committee offices, as well as support entities, such as the Legislative Counsel, and the Senate contingent of the Capitol Police. When fully deployed, the Senate COOP plan will incorporate and integrate individual contingency plans for each Senator, committee, and administrative office. Under a system of distributed decision making, each Senator or committee chair will have discretion to *activate* his or her office COOP plan as events warrant. Each office will

---

[21](...continued)
data that describe how, when, and by whom a particular set of data was collected, and how the data are formatted) generated by the legislative operations of the House. It is the House source for portions of the Legislative Information System (LIS) [http:///www.congress.gov] and Thomas, the public database of congressional information housed in the Library of Congress and available at [http://thomas.loc.gov].

[22]Bob Ney, chairman, Committee on House Administration, and Steny Hoyer, ranking member, *All Member Offices to Receive Blackberries* (sic), Dear Colleague Letter, September 21, 2001; and Bob Ney, chairman, Committee on House Administration and Steny Hoyer, ranking member, *BlackBerry Pager Update*, Dear Colleague Letter, Oct. 16, 2000. [http://www.house.gov/cha/publications/DC_s/dc_s.html].

[23]This section is based on discussions with staff in the Office of the Secretary of the Senate and the Sergeant at Arms of the Senate, and other sources, as noted.

have an office emergency coordinator (OEC) responsible for developing and maintaining the plan. The OEC will then be charged with implementing the plan.

Several units of the Secretary's office operated under their COOP plans during the Senate anthrax incident. Some offices would worked under contingency plans for a few days during the incident while others' plans were in effect for the duration of the Hart Building closure. Two such offices were the Senate disbursing office, which handles payroll operations, and the stationery office, which distributes office supplies. The offices operated from other locations while the building was unavailable. Despite the relocation, all Senate staff were paid without interruption, and office supplies were available throughout the Senate during the 3 months the building was closed.

Plans for the relocation of the Senate chamber were completed in 2002, and the Senate Sergeant at Arms and Secretary of the Senate developed a range of plans for maintaining congressional information and operations. Phase three implementation, in which leadership, committee, and Member offices were trained to develop their own COOP plans has also been completed. Under the direction of the Committee on Rules and Administration, the Sergeant at Arms and Secretary of the Senate trained leadership, committee, and Member offices to write and complete COOP plans during the spring and summer of 2002. COOP plans are dynamic, and must be reflect current operational conditions. To ensure that individual office COOP plans remain current, future Senate COOP planning will include annual awareness training for committee and officer staffs. It is also anticipated that a review of committee COOP plans by the Committee on Rules and Administration will be a part of the committee budget process in the 108th Congress. Finally, COOP plan development training will be integrated into training for newly elected Senators and their staffs at the beginning of the 108th Congress.

In addition to the formal COOP planning process, the Senate has issued BlackBerry personal digital assistants to every Senator.[24] Information technology managers in the Sergeant at Arms office have developed extensive systems for safeguarding data and electronic records, and maintain remote storage of payroll, personnel, and purchasing information through an outside vendor. Responsibility for securing and backing up committee and Member hard copy office information and computer data,[25] including e-mail and office Web sites, resides in individual offices; the Sergeant at Arms provides data backup and recovery services upon request.

---

[24]Ed Henry and Paul Kane, "BlackBerry, Anyone?," *Roll Call Daily*, Nov. 27, 2001, at [http://www.rollcalldaily.com/rollcalldaily/1_53/hoh/320-1.html].

[25]A variety of backup methods exist. One common and relatively inexpensive method for backing up data is the use of recordable compact discs (CD-R).

Current Issues and Proposals

As Congress moves forward with its COOP planning, a number of procedural, logistical, and technical issues arise. Some of these include the use of remote voting[26], information security, the compatibility between individual Member, committee, and other congressional COOP plans, and replicating traditional activities in alternative environments. Although some of these issues can be addressed by thorough planning and testing by professional staff, others, such as the possibility of remote voting, could require legislative or even constitutional responses.

Relocating Legislative Activities

Since the establishment of the District of Columbia as the national capital, Congress has been unable to use the Capitol only once. During the War of 1812, British troops burned the Capitol, forcing Congress to meet elsewhere in Washington, DC, for 5 years. In response to the recent evacuations and closures of the Capitol and House and Senate office buildings, both chambers made alternative arrangements to conduct congressional business. Some staff were able to communicate by wireless devices and e-mail systems, while others met in alternative office space or their homes. Although some Members of Congress met together informally, neither chamber met in session outside the Capitol.

During the Cold War, Congress established a remote meeting site under The Greenbrier resort in White Sulphur Springs, West Virginia.[27] The facility was reportedly established to assist Congress to carry out its activities away from Washington, DC in the event of nuclear attack. The site was equipped with facilities for House of Representatives and Senate floor activities, and a large hall to accommodate joint meetings.[28] In the absence of a national attack, this facility was never used, and has since been opened to the public for tours. At this time there are no current public proposals for the establishment of a similar facility.

The current details of physically relocating Congress are not publicly available. Congress has taken steps to authorize the relocation of floor activities, and some proposals have been put forth regarding potential facilities for Congress to use in an emergency. Under the rules of each chamber, House and Senate committee activity beyond Washington, DC, is already permissible.

Floor activity. Article I, Section 5 of the Constitution prohibits either chamber from meeting in "… any other Place than that in which the two Houses shall

---

[26]Remote voting can include a range of technology systems that might facilitate voting by Members who are not physically present on the House or Senate floor. The rules of both chambers assume that Members will be present, and do not allow remote voting. Conversely, Senate rules authorize committees to adopt rules for proxy voting, a paper based form of remote voting.

[27]See [http://www.greenbrier.com/docs/hotel_activities.html].

[28]Ted Gup, "The Ultimate Congressional Hideaway," *The Washington Post Magazine*, May 31, 1992, p. 11.

be sitting" without the consent of the other chamber.[29] There appears to be no constitutional bar, however, to the House and Senate adopting a resolution that contingently approves possible meetings of either chamber outside the Capitol in advance of any such meetings themselves. In the aftermath of the September 11 attacks and anthrax interruptions, Congress modified its adjournment resolutions to allow either chamber to reconvene at a place and time designated by the Speaker of the House and the Majority Leader of the Senate, whenever they determine the public interest shall warrant it. In making this decision, the Speaker and Majority Leader typically consult with the Minority Leaders of the House and Senate.

Some have suggested that, in the event of an interruption that renders Capitol Hill facilities unusable, Congress move to the legislative buildings of nearby state governments or other government facilities and resume operations from those locations.[30] Administrative questions COOP planners and policymakers may consider when reviewing the relocation of floor activities include, for example, what facilities are available in other locations for Members, staff and chamber officers, such as the parliamentarians, security officers, and clerks. What level of physical security exists in these facilities? If Congress chose to move to state legislative facilities, what arrangements would be necessary if the state legislature needs to hold its own legislative sessions? Some may ask whether moving Congress as a whole to another location improves security, or merely relocates a terrorist target. In practical terms, what logistical and technical issues must be addressed so that relocated floor activity can be supported at an alternative site, and within an accelerated time-frame? How would Members of Congress and staff be informed to meet at the alternative site? How would Members of Congress and staff be transported to the alternative site? What if Members of Congress were unable to get to the alternative site due to travel restrictions or interruptions? Finally, what advance arrangements would need to be made between Congress and the state legislatures that may host them?

Committees. Congressional committees hold meetings and hearings on a range of public policy issues and legislative initiatives. House Rule XI, 2 (m), states in part that a committee is authorized "... to sit and act at such times and places within the United States, whether the House is in session, has recessed, or has adjourned, and to hold such hearings as it considers necessary ...." Similarly, Senate Rule XXVI, 1, states that a committee "... is authorized to hold such hearings, to sit and act at such times and places during the sessions, recesses, and adjourned periods of the Senate ..." as it sees fit.[31] Funding for committee travel and guidelines on other

---

[29]In the House, "place" has been interpreted to mean the seat of government. See U.S. Congress, House, *Constitution, Jefferson's Manual and Rules of the House of Representatives of the United States, 107th Congress*, H. Doc. 106-320 106th Congress, 2nd session, compiled by Charles W. Johnson, Parliamentarian. (Washington: GPO, 2001), pp. 34-35. By statute, the seat of government is anywhere within the boundaries of Washington, DC. See 4 U.S.C. 71.

[30]Amy Keller, "E-Congress: Possible? Yes. Likely? No." *Roll Call*, Nov. 5, 2001, p. A1.

[31]Under meetings of committees, *Riddick's Senate Procedure* also states that each Senate standing committee or their subcommittees "... is authorized to hold hearings, to sit and act at such times and places during the sessions, recesses, and adjourned periods of the (continued...)

administrative matters involved in hearings away from the Capitol are already established by regulations issued by the House Administration Committee and the Senate Rules and Administration Committee.[32]

Electronic Sessions and Legislation in the 107th Congress

The events of September 11, 2001, and the subsequent anthrax incidents have highlighted some of the potential vulnerabilities of the centralized assembly of the nation's lawmakers, prompting some observers to suggest creating a virtual or electronic Congress (e-Congress). In the 107th Congress (2001-2002) a proposal (H.R. 3481) was been introduced to require the National Institute of Standards and Technology (NIST) to investigate the feasibility and costs of implementing a computer system for remote voting and communication for Congress to ensure business continuity for congressional operations. The Committee on House Administration held hearings on e-Congress initiatives and other issues surrounding the continuity of congressional operations on May 1, 2002. A second measure (H.R. 5007) was introduced, directing the Comptroller General to enter into arrangements with the National Academy of Science and the Librarian of Congress to examine the feasibility and costs, and the constitutional and procedural issues associated with the creation of an emergency electronic communication system for Congress, respectively. In a press release announcing his intention to introduce the H.R. 3481, Representative James Langevin, who sponsored both measures, cited the importance of maintaining "the effective operation of the nation's highest lawmaking body," as well as the need to "learn from our mistakes and take the necessary steps to prepare for future threats to ensure that government can continue to conduct its business effectively."[33]

Although it is unclear exactly how an e-Congress would be constituted and operated, some observers have offered some broad suggestions involving the establishment of a Web site that Members could access from anywhere in the country (and perhaps the world).[34] Proponents envision such a Web site would enable

---

[31](...continued)
Senate..." Floyd M. Riddick and Alan S. Frumin, *Riddick's Senate Procedure: Precedents and Practices*, S. Doc. 101-28 (Washington: GPO, 1992), p. 404. Discussion with the House parliamentarian indicates that the chair in the House has never been called upon to rule on the matter of House committees holding meetings beyond Washington, DC.

[32]In the House, regulations printed in the House Administration Committee's Congressional Handbook cover matters specific to field hearings. The handbook is available from the committee and can be viewed online at [http://www.house.gov/cha/cmtehdbkcover.html]. In the Senate, committee travel in general is governed by regulations compiled in the U.S. Senate Handbook (Chapter 11, Appendix D of the 1996 edition). Print and online versions of the handbook are available - to Senate offices only - from the Senate Committee on Rules and Administration.

[33]For the full text of the press release, see [http://www.house.gov/apps/list/press/ri02_langevin/pr120601continuity.html].

[34]Amy Keller, "E-Congress: Possible? Yes. Likely? No." *Roll Call*, Nov. 5, 2001, p. A1; J.H. Snider, "Planning for the Worst," *Federal Computer Week*, Oct. 15, 2001, p. 36; Noah (continued...)

Members to carry out activities normally done on the chambers' floors or in committees. The possibility of convening an e-Congress raises a number of procedural, technical, and resource questions, some of which have not yet been addressed. A more complete discussion of issues raised by the development of an electronic Congress can be found in CRS Report RS21140, *Electronic Congress: Proposals and Issues*.

Member Office Information Security

Continuity planners suggest that a critical element of COOP planning is to plan ahead and to develop a clear understanding of what materials and information are most crucial to continuing operations if regular facilities are not available.[35] A component in this planning is the preservation of critical information maintained in computer systems.

Congressional offices that wish to retain control over their own data may prefer to develop their own plans for backup and subsequent recovery of critical information recorded on paper and electronic media. Information security professionals recommend making a regular, global backup of system files and data, and more frequent (daily) backups of new and recently changed files. This might include systematic scanning and retention of electronic images of irreplaceable paper documents.[36] Backup copies then need to be stored in a secure location other than the office where the original files are located. For example, Member Capitol Hill offices could store backup copies in state or district offices, and vice versa. Information security professionals also recommend additional actions such as maintaining a series of regularly updated copies, so that not all office data are lost in the event that a particular backup copy is corrupted, or otherwise compromised by a virus, defective media, or other cause.[37]

---

[34](...continued)
Shachtman, "Can Congress Convene Online?" *Wired News*, Oct. 25, 2001, [http://www.wired.com/news/politics/0,1283,47841,00.html].

[35]See James Schultz, "New Urgency for Disaster Recovery Planning," *Washington Technology*, Oct. 8, 2001, pp. 18-20.

[36]Despite many predictions regarding the advent of the so-called paperless office, the blizzard of paper that accompanied the dust and debris with the collapse of the World Trade Center towers on Sept. 11, 2001 suggests many organizations are still heavily dependent on their physical documents. One company that did have a comprehensive digital imaging system in place before Sept. 11 was Empire Blue Cross Blue Shield. Developed over the past 10 years, starting with claims forms, the insurance carrier's optical storage system captures almost all of its paper documents. As a result, the company lost only about 2 days' worth of paper mail. See Stan Gibson, "Rethinking Storage," *eWeek*, Oct. 15, 2001, p. 1.

[37]See Lisa Yeo, "SOHO Security Best Practices," at
[http://www.sans.org/infosecFAQ/homeoffice/SOHO.htm].

Additional Considerations

As COOP projects move forward, planners may also continue to consider responses to the possibility of interruptions affecting critical operating systems and data such as communications, the Legislative Information System (LIS), and individual Member computer resources. An electronic interruption or cyber attack could manifest itself through the spread of computer viruses or worms. It could also take the form of hackers gaining access to congressional computer systems or denial-of-service (DoS) attacks on congressional Web servers.[38] Similarly, another possibility is an attack, physical or electronic, or other interruption to a major telecommunications switching station in the Washington, DC, area, which could significantly affect the Congress's ability to communicate both internally and externally. Some of these vulnerabilities are being addressed through the implementation of wireless devices, such as the BlackBerry.[39]

Selected Glossary of COOP-Related Terms[40]

Action Officer - designated individual with the responsibility to ensure that all actions prescribed to his/her respective department/office are executed according to the policies and procedures of the COOP.

After-Action Report (AAR) - a narrative report that presents issues found during an incident and recommendations on how those issues can be resolved.

Alternate Database/Records Access - the safekeeping of vital resources, facilities, and records, and the ability to access such resources in the event that the COOP plan is put into effect.

Alternate Facilities - an alternate work site that provides the capability to perform minimum essential department or office functions until normal operations can be resumed.

Art and Other Valuables - Objects of art, including photographs, paintings, lithographs, statuary, rugs, tapestries, books and similar items that are on loan from an individual or institution or are personal property of the Senator or staff.

Business Continuity - the sum of an organization's business. It includes all of the core business functions, which define the organization. A business continuity plan includes risk mitigation strategy, contingencies, and recovery, to ensure the

---

[38]A denial-of-service attack is an attempt to crash a network or make a Web site inaccessible by flooding it with useless traffic.

[39]For an overview of potential electronic incursions, see Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," at [http://www.terrorism.com/documents/denning-infoterrorism.html].

[40]This glossary was excerpted from the Continuity of Operations Plan 2002 template used for training and plan development purposes by the Sergeant at Arms of the Senate.

organization's core business processes continue despite disruptions to infrastructure or support systems.

Business function - a group of logically related tasks that are performed together to accomplish an objective.

Business priority - is derived by the combination of risk assessment and impact. The priority can help the organization determine areas of emphasis and where resources will be employed when it becomes obvious not all risks can be mitigated.

Business Resumption Team - a team comprising application system expertise and business analysts. This is a quick action team that will pinpoint a problem and be equipped/trained to correct the problem and restore operations, at least minimally.

Cold Site - a relocation site that is reserved for emergency use, but which requires the installation of equipment, etc., before it can support operation.

Continuity of Government (COG) - applies to the measures taken by the government to continue to perform required functions during and after a severe emergency. COG is a coordinated effort within each branch of the government to continue its minimum essential responsibilities in a catastrophic emergency.

Continuity of Operations (COOP) - an internal effort within individual components of the executive, legislative and judicial branches of government to assure the capability exists to continue essential component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

Emergency - a sudden, usually unexpected event that does or could do harm to people, resources, property, or the environment. Emergencies can range from localized events that affect a single office in a building, to human, natural or technological events that damage, or threaten to damage, local operations. An emergency could cause the temporary evacuation of personnel or the permanent displacement of personnel and equipment from the site to a new operating location.

Emergency Personnel - any person whose presence on-site is deemed necessary in a situation or an occurrence of a serious nature, which develops suddenly and unexpectedly, and demands immediate action.

Essential Functions - those functions, stated or implied, that are required by the Leadership to be performed by the SAA, to provide vital services, maintain the safety and well being of the Senate community and general populace, and continue to fulfill the constitutional obligations of the Senate.

Essential Operations - those operations, stated or implied, that are required by the Leadership to be performed by the SAA.

Essential Positions - those positions, stated or implied, that are required to be filled by the SAA or other positions deemed essential by the Senate Leadership.

Fly-Away Kit - an easily transported set of materials, technology, and vital records that will be required to establish and maintain minimum essential operations.

Hot Site - a relocation site available for immediate occupancy that is equipped to permit rapid resumption of essential functions.

Internet - worldwide interconnection of computers, typically interconnected using the TCP/IP protocol. Access to the Internet is normally through service providers and available to the general public.

Interoperable Communications - alternate communications that provide the capability to perform minimum essential department or office functions until normal operations can be resumed.

Intranet - a privately operated internal computer network that is used to publish information, and implement human resource or other business applications within a company or organization. Intranets normally provide services to staff and other individuals within a company or organization.

Logistics Team - a working group responsible for coordinating the activities associated with relocation planning and deployment of essential operations and positions during a COOP event.

Management Plan - an operational guide that ensures the implementation, maintenance, and continued viability of the COOP.

Office Emergency Coordinator (OEC) - Individual responsible for implementing the office or committee COOP plan during an emergency.

Plan Maintenance - steps taken to ensure the COOP plan is reviewed annually and updated whenever major changes occur.

Primary Facility - the site of normal, day-to-day operations; the location where an employee usually goes to work.

Rights and Interest Records - records required for the preservation of the rights and interests of individual citizens and the government. These records include proof of ownership, financial interests, and legal proceedings and decisions. Rights and interest records are not generally believed to be needed during an emergency.

Relocation Site - the site where all or designated employees will report for work if required to move from the primary facility.

Situation Report (SITREP) - a written, formatted report that provides a picture of the response activities during a designated reporting period.

Special Reconstitution Teams - a group of several individuals who together may be assigned specific responsibilities to manage and support the SAA's requirements during the initial phase of a COOP event. Examples of these teams are: Logistics, Damage Assessment, and Employee Tracking.

Training and Exercise - this activity includes: (1) efforts to educate/advise designated staff on COOP responsibilities, and on the existing plans; and (2) tests to demonstrate the viability and interoperability of all plans supporting COOP requirement.

U.S.P.S. - United States Postal Service.

Vital Records and Systems - records necessary to maintain the continuity of operations during an emergency, to recover full operations following an emergency, and to protect the legal rights and interests of citizens and the government.

Working Documents - documents that enable or facilitate office operations but are not legally required for departmental operations.

Additional Reading

CRS Report RS21140, *Electronic Congress: Proposals and Issues*, by Jeffrey W. Seifert and R. Eric Petersen.

CRS Report RS21089, *Continuity of Government: Current Federal Arrangements and the Future*, by Harold C. Relyea.

CRS Report RS21068, *House Vacancies: Selected Proposals to Allow for Filling Them Due to National Emergencies*, by Sula P. Richardson.

CRS Report RS20928, *Field Hearings: Fact Sheet on Rules, Regulations, and Guidelines*, by Richard C. Sachs.

CRS Report RS20272, *FEMA's Mission: Policy Directives for the Federal Emergency Management Agency*, by Keith Alan Bea.

CRS Report RL31103, *House of Representatives Information Technology Management Issues: An Overview of the Effects on Institutional Operations, the Legislative Process, and Future Planning*, by Jeffrey W. Seifert and R. Eric Petersen.

CRS Report RL30861, *Capitol Hill Security: Capabilities and Planning*, by Paul E. Dwyer and Stephen W. Stathis.

CRS Report RL30699, *Nuclear, Biological, and Chemical Weapons and Missiles: The Current Situation and Trends*, by Robert Shuey.

CRS Report RL30735, *Cyberwarfare*, by Steven A. Hildreth.

CRS Report 98-731, *Presidential and Vice Presidential Succession*, by Thomas H. Neale.