Order Code RL31103

Report for Congress
Received through the CRS Web

House of Representatives Information Technology Management Issues: An Overview of the Effects on Institutional Operations, the Legislative Process, and Future Planning

Updated April 2, 2003

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

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

House of Representatives Information Technology Management Issues: An Overview of the Effects on Institutional Operations, the Legislative Process, and Future Planning

Summary

In the past decade, information technology (IT) has become an integral part of managing governance at the local, state, federal, and international levels. In the House of Representatives, computers, telecommunications, and video technologies have become pervasive. While some systems have been in existence for many years, the technological changes of the past few years represent an exponentially greater change in congressional operations compared to the previous two decades. Today, the House of Representatives relies heavily on IT to improve the efficiency of its internal operations, to enhance Member and staff access to information useful in the legislative process, and to facilitate the production of legislative documents. These changes support the House of Representatives' transition into the electronic government (e-government) environment. However, as IT has become more integrated into House operations, attention is shifting toward issues related to IT staffing, emergency communications, and continuity of operations (COOP) planning.

Before 1995, the House of Representatives was essentially a paper-based institution. Since that time, IT infrastructure improvements have provided high speed Internet and network access to all House offices, and improved information security protections, among other advances. Public access to congressional information has also been enhanced through the development of THOMAS, the House of Representatives Web site, and the use of digital audio and video transmissions for some hearings.

While increased IT use in the House of Representatives has yielded benefits, it has also raised issues, both in terms of the effects on the legislative process and the future development of IT initiatives in the House of Representatives. The outcome of future IT initiatives will be partly dependent upon the resolution of emerging issues such as technology management; security and authentication concerns; changes in document publishing distribution; archiving; and staffing issues.

This report considers the institutional impact of integrating IT in the House of Representatives on operational and management issues. It includes an overview of ongoing initiatives to upgrade the technological infrastructure of the House of Representatives as well as efforts to enhance public access to congressional information, and ensure the continuity of operations in the event of a disruption. The report also explores the effect of IT on the administration of Member offices, committee operations, and the legislative process. The report concludes with a review of developing technology issues facing the House of Representatives as it continues to implement its IT strategy. A glossary of relevant IT and e-government terms is also included.

Contents

House of Representatives Information Technology Management Issues: An Overview of the Effects on Institutional Operations, the Legislative Process, and Future Planning

Introduction

In the past decade, information technology (IT) has become an integral part of managing governance at the local, state, federal, and international levels. In the House of Representatives, computers, telecommunications, and video technologies have become pervasive. While some systems, such as electronic voting, video coverage of floor proceedings, and legislative information tracking, have been in existence for many years, the technological changes of the past few years represent an exponentially greater change in congressional operations compared to the previous two decades. Today, the House of Representatives relies heavily on IT to improve the efficiency of its internal operations, to enhance Member and staff access to information useful in the legislative process, and to facilitate the production of legislative documents. These changes have equipped the House of Representatives to enter the electronic government (e-government) environment.

The growth of IT presents a variety of opportunities, challenges, and concerns regarding the administration of the House of Representatives and the legislative process. The use of personal computers and computer networks has an impact on the way offices operate, information is shared, and individuals communicate. These systems may also make it possible to approach existing institutional and legislative operations in new ways. The use of advanced IT has become a major factor among a variety of social, demographic, and political trends that influence the political process. Among the biggest challenges for the House of Representatives is adapting IT in ways that conform to the rules and traditions of the chamber.

This report examines the institutional impact of integrating IT in the House of Representatives on operational and management issues. It includes an overview of ongoing initiatives to upgrade the technological infrastructure in Member offices and committees of the House of Representatives as well as efforts to enhance public access to congressional information. The report also explores the effect of IT on the legislative process. The report concludes with a review of developing technology issues facing the House of Representatives as it continues to implement IT systems. A glossary of relevant IT and e-government terms is also included.

House Information Technology Oversight Responsibility and Management

Management and oversight responsibility for IT in the House of Representatives is dispersed among several officials and entities that typically work in concert to develop and implement policy and procedures. The Speaker has general control of the part of the Capitol assigned to the House of Representatives.[1] The House of Representatives elects several officers; two of those officers, the clerk and the chief administrative officer (CAO) have primary IT responsibilities. The clerk is responsible for maintaining a record of chamber proceedings, examination of all legislative measures, and the management of other House of Representatives documents.[2] The CAO is charged with operational responsibility for functions as assigned by the Committee on House Administration. The clerk and CAO may be removed by a vote of the House membership, or, unilaterally, by the Speaker.[3] At the beginning of the 107th Congress, the Committee on House Administration was given authority to "provide policy direction for the Inspector General and oversight of the Clerk, Sergeant-at-Arms, Chief Administrative Officer, and Inspector General."[4] The Committee on Appropriations Subcommittee on Legislative provides formal and informal guidance in matters of IT management through the annual legislative branch appropriations process.

Operational responsibility for IT services is divided between the Office of the Chief Administrative Officer and the Office of the Clerk. The CAO administers IT services through the Office of House Information Resources (HIR). HIR provides information systems support for Members, committees, and administrative offices of the House of Representatives. It coordinates computer hardware, software, and telephone equipment support services with commercial vendors, and provides direct support for systems integration, implementation, and development. Additionally, HIR provides consultation services for the acquisition of computer equipment,

---

[1] Rule I (3) of the House of Representatives, in U.S. Congress, House, *Constitution, Jefferson's Manual and Rules of the House of Representatives of the United States, 107th Congress*, (hereafter *House Rules and Manual, 107th Congress*) H. Doc. 106-320 106th Congress, 2nd session, compiled by Charles W. Johnson, Parliamentarian. (Washington: GPO, 2001), p. 333.

[2] Rule II (2) of the House, in U.S. Congress, House, *House Rules and Manual, 107th Congress*, p. 345.

[3] Rule II (1) of the House, ibid.

[4] Sec. 2 (g) 1, H. Res. 5, (107th Congress), *Adopting rules for the One Hundred Seventh Congress*, adopted January 3, 2001. In the notes following Rule X (2), at § 728, the Parliamentarian indicates that "in the 107th Congress the Committee [on House Administration] retained the responsibility to provide policy direction to and oversight of the Inspector General but retained only oversight of the remaining officers" of the House, including the CAO. See U.S. Congress, House, *House Rules and Manual, 107th Congress*, p. 437.

troubleshooting, computer security services, and training in application software and operating systems.[5]

In the Clerk's office, the Legislative Computer Systems (LCS) office is responsible for developing and managing paper and electronic content relating to legislative and floor activities. Systems and services which fall into this category include the Legislative Information System (LIS) and the Legislative Information Management System. Each of these systems tracks legislative measures and documents at all stages of the legislative process.

Evolution and Utilization of Information Technology in the House of Representatives, 1995-2003

Coinciding with the popular growth of the Internet and the systematic integration of IT services in other areas of the federal government, as well as the private sector, the House of Representatives in 1995 began the transition to a multimedia information environment. Previously, House of Representatives electronic documents that did exist, including successive versions of legislative information, committee reports, and other legislative branch documents, all were maintained on separate computer systems. Most documents were only available for mass distribution in hard-copy format. No common computer platforms existed, and there was no common architecture, language, or format by which information could be easily integrated, shared, electronically distributed, or viewed among offices or organizations. Access to most legislative information was accomplished through the use of computer equipment accessing a mainframe program. Electronic mail (e-mail) and other computing systems were available in some Member and committee offices, but there was no overarching approach to the use of IT.

To address these issues, the leadership of the incoming majority of the 104th Congress began to develop a blueprint for integrating IT into House operations. A multi-phased plan, the blueprint emphasized the development of internal systems to provide all House offices with appropriate information infrastructure to take advantage of advances in electronic and communications technologies. Another goal was the provision of public online access to legislative information by the opening of the 104th Congress and the creation of an array of systems to increase public access to congressional operations. The Committee on House Oversight[6] was charged with the development of the project.[7]

---

[5] U.S. Congress, House, *House Smart: House Reference Guide to Information and Services*, 106th Congress, 1st session (Washington, 1999), p. 9.

[6] From its creation under the Legislative Reorganization Act of 1946 through the 103rd Congress, the committee was called "House Administration". The committee existed under the name "House Oversight" during the 104th and 105th Congresses. At the beginning of the 106th Congress, the name changed to the "Committee on House Administration."

[7] For a historical overview of IT integration in the House, see David Dreier, chairman, Committee on Rules, *We've Come a Long Way...Maybe*, (continued...)

Internal Information Technology Operations

In February 1995, the House Oversight Committee established a Computer and Information Systems Working Group to undertake a comprehensive study of all House computers, networks, and user requirements. The formal *House Information Systems Program Plan* developed by the working group was adopted by the House Oversight Committee in November 1995. The plan called for a "robust, coherent, unified multimedia network, with sufficient software and modern compatible equipment, with which the U.S. House of Representatives may effectively function to best serve the American public, the Members of the House, and other government institutions." The implementation of this plan was popularly referred to as the "CyberCongress" project. The plan called for:

- Infrastructure upgrades of the House network;
- Replacing outdated computer hardware and software with advanced desktop computers and fully integrated office systems software capable of handling information in text, audio, and video formats;
- Developing a comprehensive security program for the House of Representatives to ensure the integrity and authenticity of electronic information;
- Improving support and training;
- Developing an Internet presence on the World Wide Web for the House of Representatives, including public access to House documents and public e-mail from constituents to their Representatives;
- Implementing new computer applications and technologies to support House operations; and
- Collaboration among all legislative branch organizations to develop joint research capabilities to support Members and committees.[8]

Additional impetus for technological innovation in the House of Representatives emanated from the recommendations of a series of information systems management audits that grew out of the 1995 House-wide independent audit conducted by PricewaterhouseCoopers (PWC). Based on the results of these audits, the Office of

---

[7](...continued)
[http://www.house.gov/rules/congress_andthe_internet.pdf]; and U.S. Congress, House, Committee on House Oversight, *Report on the Activities of the Committee on House Oversight of the House of Representatives During the One Hundred Fourth Congress*, House Report 104-885, 104th Congress, 2nd session, (Washington: GPO, January 2, 1997), pp. 3-4.

[8] *CyberCongress Accomplishments During the 104th Congress*. Presented by the Computer and Information Services Working Group to the Committee on House Oversight, February 11, 1997.

the Inspector General of the House of Representatives issued several reports on various aspects of the body's information systems environment. The CAO used the audits' recommendations as guidance to develop strategies to address issues related to physical technology infrastructure, computer security, management of technology systems life cycles, and a range of other IT issues.[9]

Infrastructure Development.[10] Planning to integrate IT systems into congressional operations included extensive upgrades of infrastructure, changes in House procurement rules, and ongoing management of upgraded and emerging technologies.

A multi-year project was initiated in 1995 to upgrade the wiring infrastructure of the House of Representatives to support higher performance and new application requirements. By 1999, all House offices had access to high-speed transmission facilities and multimedia capabilities. This permitted Members of Congress, committees, and congressional leadership offices to deploy emerging audio and video technologies. Additionally, Washington, D.C. and district offices were integrated into CapNET, Capitol Hill's wide area network that was expanded to support both Internet and secure dial-in access.

In order to take full advantage of this technical infrastructure upgrade, a strategy was developed to integrate all databases, computers, networks and vendor services throughout the House information systems environment. A component of this effort was the reorganization of the Office of House Information Systems (HIS). The renamed Office of House Information Resources (HIR) comprised four divisions: Client Services, Communications, Operations, and Integration.

In recent years, the CAO has initiated several new programs to maintain and upgrade the information infrastructure of the House of Representatives, and to increase the robustness and reliability of the House computer networks and e-mail systems. The CAO upgraded the software running the House messaging system to handle increased volume, improve virus protection, and achieve a 99% availability "up time" during 2000. The available bandwidth for Internet access in the House of Representatives was more than doubled from 10 megabyte (Mb) to 21 Mb per second.

Remote connectivity was also improved by adding faster dial access capability, enabling Members and their staffs to access information and communications while

---

[9]U.S. Congress, House, Office of Inspector General, *Audit Report: House Computer Systems Were Vulnerable to Unauthorized Access, Modification, and Destruction*, Report No. 95-CAO-18, July 18,1995*; Audit Report: The Management and Control of the House's Information Systems Operations Should be Improved to Better Meet Member's Needs*, Report No. 95-CAO-19, July 18,1995; and *Audit Report: The House Needs to Follow a Structured Approach for Managing and Controlling System Development Life Cycle Activities of its Computer Systems*, Report No. 95-CAO-20, July 18,1995. These reports are available at [http://www.house.gov/IG/page2.htm].

[10]Parts of this section are based on information provided by the Office of House Information Resources (HIR), and other sources, as noted.

traveling on congressional business.[11] In addition, efforts to enhance connectivity for district offices were also continued through a successful pilot project using digital subscriber line (DSL) technology[12] to connect district offices to the Washington, D.C. campus data network. End-user support was also increased through the introduction of the HIR Call Center in February 1999,[13] ongoing training courses, and the initialization of the Correspondence Management System (CMS)[14] evaluation program.

In August 2001, the Chairman and the Ranking Member of the Committee on House Administration announced plans to upgrade the Campus Data Network (CDN) which connects district offices to House of Representatives information resources based in Washington, D.C. In addition to enhancing the speed and reliability of network resources, the committee also made a virtual private network (VPN) service available to House offices. The VPN utilizes encryption technology to enable private and secure communications for single-person district offices, telecommuters and House staff. User may access the CDN through the VPN using high-speed

---

[11]This was accomplished using V.90 analog modems and integrated services digital network connections (ISDN). V.90 is a technical standard, approved by the International Telecommunication Union, used for 56 kilobits per second (Kbps) modems. ISDN is an international communications standard utilized for sending voice, video, or data over either digital or copper telephone lines at data rates up to 128-Kbps.

[12]DSL technologies use sophisticated modulation schemes to compress data using standard copper telephone wires, providing high-speed Internet access.

[13]The call center received and responded to 66,556 calls during the 106th Congress.

[14]According to the Congress Online Project, correspondence management systems are "database programs specifically designed to help House and Senate offices record, process, track, and manage their constituent correspondence. Almost all House and Senate offices use correspondence management system (CMS) databases to manage the thousands of postal letters, e-mail messages, phone calls, and faxes they receive from and send to constituents each year." [http://www.congressonlineproject.org/glossary.html#C]. The Congress Online Project is a two-year program funded by The Pew Charitable Trusts and conducted jointly by the George Washington University and the Congressional Management Foundation (CMF) to examine the use of Web sites and other forms of online communications by congressional offices.

connections, SecurID cards[15] and the Internet.[16] In April 2002, it was reported that 36 district offices and 172 individual staff members were using the VPN.[17]

Desktop Computer Upgrades. To deliver the technology to the desktops of users, the CAO in 1995 oversaw changes to procurement procedures for computer-related equipment. A decision was made to eliminate the previously used "approved list" of office equipment for the House of Representatives. In June 1999, the Committee on House Administration approved the CAO's proposal to adopt a formal Systems Development Life-Cycle (SDLC) process to guide future technology projects. Under new guidelines, offices could use official expenses to buy any computer hardware and software that met minimum quality standards set by the CAO. By 2000, 12,000 computers had been replaced. All workstations are now connected to a network that features Internet access and a single House-wide e-mail messaging system, and have replaced several smaller and mutually incompatible systems. The Committee on House Administration currently recommends that offices upgrade computers that run the Windows 98 and Windows NT operating systems before Microsoft Corporation ends support for those platforms in June, 2003.[18]

Security. The 1995 PWC audit report, and a review by the House inspector general, identified internal deficiencies that could place Member services at risk. The audit report noted a lack of security planning to protect House computers and networks against tampering and data loss. Weaknesses were noted throughout all processing environments, including HIR operations and office level systems.

In response to guidance from the Committee on House Oversight based on the audit's recommendation, HIR began implementing corrective actions in 1995 to address all recommendations. Examples of these initiatives included:

- exploring the feasibility of implementing enhanced encryption for House e-mail systems;

---

[15] SecurID is a cryptographic smart card personalization system that enables a single card to be programmed for network access, digital credentials, physical building access and identification. It is manufactured by RSA Security, Inc.

[16] Bob Ney, chairman, Committee on House Administration, and Steny Hoyer, ranking member, *Virtual Private Network (VPN) Connectivity for Single-Person District Offices and Private Residences*, Dear Colleague letter, December 10, 2001 [http://www.house.gov/cha/December_10.htm]; U.S. Congress, House, Committee on House Administration, "House Administration Speeding Up District Office Network Connection," committee press release, August 3, 2001; "House to Get Faster Computer Network," *Government Executive Magazine*, August 21, 2001 [http://www.govexec.com/dailyfed/0801/082101cd.htm]; "House Speeding up Network," *Federal Computer Week*, August 28, 2001 [http://www.fcw.com/fcw/articles/2001/0827/web-house-08-28-01.asp].

[17] Jason Miller, "House VPN Connects Staff Remotely," *Government Computer News*, April 29, 2002, p. 13.

[18] Bob Ney, chairman, Committee on House Administration, and Steny Hoyer, ranking member, *Minimum Supported Technical Standards*, Dear Colleague letter, July 31, 2002.

- revising security guidelines, including appropriate physical and environmental controls over desktop and in-office systems;

- periodic security audits and security consultations with Member and committee offices;

- requiring vendors to ensure that system access controls could not be circumvented; and

- reviewing and implementing more stringent security controls over House information systems.

In response to possible susceptibility of the House e-mail system to outside infiltration, a "House E-mail Support Team" was formed in HIR to monitor the system more closely. In 1998, the committee issued a document detailing security guidelines for protecting IT systems from unauthorized use. These guidelines were revised and updated in October 2000. The purpose of the guidelines is to provide Member, committee, and administrative offices with a policy governing general security requirements for using House computing and network information systems.[19]

A number of other IT security policies have been approved by the Committee on House Administration in the past few years. These include rules governing the protection of Member and committee office systems, Internet and intranet security,[20] wireless network security, and policies governing the response to information system-related security incidents, and remote access to the House network by vendors.[21] In addition, the Information Systems Security Group in HIR created an intranet site to distribute security information, including general security measures, and procedures for configuring computers in accordance with security standards.[22]

---

[19] U.S. Congress, House, Committee on House Administration, "The United States House of Representatives General Information Security Guidelines for Protecting Systems from Unauthorized Use," HISPOL 002.0, Issued, February 4, 1998, revised, October 17, 2000. Available internally at [http://onlinecao.house.gov/hir-security/hisdoc.htm].

[20] An intranet is a network based on TCP/IP protocols belonging to an organization, such as a corporation or agency, that is accessible only by the organization's members, employees, or others with authorization. In essence, an intranet functions like an internal internet that is not accessible to the general public.

[21] See U.S. Congress, House, Committee on House Administration, "Protection for Member and Committee Office Systems from Unauthorized Use," HISPOL 002.1; U.S. Congress, House, Committee on House Administration, "Internet/Intranet Security Policy," HISPOL 003.0; U.S. Congress, House, Committee on House Administration, "Information Security Policy for Information System-Related Security Incidents," HISPOL 004.0; and U.S. Congress, House, Committee on House Administration, "Information Security Policy for Vendor Remote Access to the House Network," HISPOL 005.0; U.S. Congress, House, Committee on House Administration, "The United States House of Representatives Wireless Network Security Policy," HISPOL 006.0. All documents are available on the Internet, internally at [http://onlinecao.house.gov/hir-security/hisdoc.htm].

[22] The House security information Web site can be found at [http://onlinecao.house.gov/hir-

Other recent security efforts have included the registration of Web server Internet protocol (IP) addresses with HIR's Information System Security Office;[23] the implementation of a firewall strategy; a House-wide system security audit program; the completion of the Information Systems Security Program (ISSP), which provides the framework for the House IT security strategy; and ongoing upgrades in virus protection software and procedures.[24] In addition, the Office of Legislative Counsel recently began using biometric[25] authentication software to safeguard its files and information.[26]

HouseNet - The House Intranet. As part of the deployment of IT services, the House of Representatives established HouseNet, the House intranet [http://housenet.house.gov/] as a one-stop online information resource.[27] Accessible through a Web browser, the private network features links to a House e-mail address database, House news and schedule information, House officers' pages, external information services, and a selection of House operations publications.

House Information Resources Training and Support. Through House Information Resources (HIR), the CAO has initiated an extensive IT training program and support system for the House. Technical training programs provide instruction in common office applications, Web languages, systems administration, and legislative research. Specific courses are offered in a variety of formats, including instructor led training, and self study through CD-ROM and videotape-based tutorials. In addition, many of the training opportunities are available online to support House district staff. HIR also provides help desk services for user inquiries, as well as a range of Web support services to assist offices to manage constituent e-mail, online press release updates, and Web site design and hosting. A listing and descriptions of the programs offered, is available on HouseNet through the "Employee Benefits" link.

---

[22](...continued)
security/].

[23]The registration is designed to keep computers not designated for Web access from being attacked from outside the system.

[24]Bob Ney, Chairman, Committee on House Administration, *New Computer Anti-Virus Protection for the House*, Dear Colleague Letter, January 23, 2001; and Bill Thomas, Chairman, Committee on House Administration, *Reinforcing Security of Office Servers*, Dear Colleague Letter, June 20, 2000. These documents are available at [http://www.house.gov/cha/publications/publications.html].

[25] In computer security, biometrics refers to authentication techniques that rely on measurable physical characteristics, such as fingerprints, voice patterns, or retinas, that can be automatically verified.

[26] Gail Repsher Emery, "House Office Picks Saflink's Biometric Software," *Washington Technology*, May 31, 2002, at [http://www.washingtontechnology.com/news/1_1/daily_news/18365-1.html].

[27]Although the House intranet has existed for several years, it was recently renamed HouseNet.

Legislative Information System (LIS). In conjunction with the Senate, Library of Congress (LOC), and the Congressional Research Service (CRS), the House Oversight Committee developed a coordinated strategy for deploying a single, integrated system to organize information from the existing unconnected House and Senate systems[28] as well as from other legislative branch agencies, including the General Accounting Office (GAO) and the Government Printing Office (GPO). This effort resulted in the creation of the Legislative Information System (LIS) [http://www.congress.gov/] in the 105th Congress. LIS provides Members, committees, leadership offices, and legislative branch agencies with a wide range of legislative information. An enhanced version of the publicly available THOMAS (described below), LIS is available only to legislative branch offices. The system includes access to the text and status of legislation; the *Congressional Record*; committee reports and hearing transcripts; analyses from the CRS, the Congressional Budget Office (CBO), and GAO; and links to commercial information sources.

Committees. Committees on an individual basis have also been involved with the integration of IT. An example of intensive use of IT systems can be found in the hearing rooms of the Committee on Science. During the 106th Congress, the committee upgraded the technical infrastructure of one of its hearing rooms to enable greatly enhanced multi-media capabilities. Each Member's dais area includes audio and data ports for computer access to the House system. The hearing room has three wall-mounted cameras, a retractable projector mounted in the ceiling, a drop-down screen for Member viewing, flat screen monitors for audience and witness viewing, and a touch-screen monitor at the chairman's seat to view computer generated presentations, video, or cable TV (CATV). In addition, an operator's console is capable of video conferencing, overhead projection, mounting prepared presentations on a laptop, audio and video tape presentation and recording, Digital Versatile Disc (DVD) presentation, access to the Internet, and distribution of live audio/video feeds via the committee's Web page. A second hearing room is equipped to act as an overflow room, and has a subset of the above audio and video capabilities.[29] Similar upgrades are being considered or installed in facilities used by other committees as part of the committee hearing room upgrade project overseen by the Committee on House Administration.

One overall consequence of the wider use of IT is that it has served to make committee activity more accessible to a wider audience. Many committees request that witnesses provide their testimony electronically as well as in printed form so that it can be quickly made available on their Web sites. Some committees also provide access to hearing transcripts on their Web sites. By the end of the 107th Congress, several committees had begun to provide audio coverage of their hearings over the Internet. The Committee on Financial Services has since June 2002 also made available a video feed of its proceedings. Users have the option of watching committee activities live in a overflow room in the Capitol Complex, or over the

---

[28]In the 103rd Congress, four overlapping legislative tracking systems existed: the House's LEGIS and ISIS systems, Senate LEGIS, and the Library of Congress SCORPIO system.

[29] Information provided by the House Committee on Science, April 12, 1999.

Web with video on demand technology.[30] At its inaugural hearing during the 108th Congress, the Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census became the first House subcommittee to implement video to text technology in a hearing. Using an advanced database that combines voice recognition with transcription capabilities, the video to text application enables the user to search for keywords and phrases. The results of the search can then either be viewed as a short video clip, or in text form.[31]

Electronic Mail. According to a report by the Congressional Management Foundation and The George Washington University, the number of e-mail messages received by the House of Representatives increased from 20 million in 1998 to 48 million in 2000.[32] Following the disruption to postal mail in the aftermath of the anthrax incidents in 2001, the House began receiving approximately one million e-mail messages daily.[33] Overall, the House received 78% more e-mail in 2001 compared to 2000. However, the rate of increase for 2002 appears to have leveled off significantly, to a projected rate of 2.5%, based on data from the first six months of the year.[34] Two primary reasons are attributed to the stabilization of e-mail traffic to the House of Representatives. One reason is the use of enhanced filters and other anti-spam techniques. The second reason is the increased use of Web-based forms, which can help screen out non-constituent mail and organize incoming messages according to issue, topic, or other means.[35]

Electronic Document Management System. Another component of the ongoing effort to enhance the use of technology for legislative operations in the House of Representatives is the implementation of the House Electronic Document Management System (DMS). The goal of this enhanced technology is to make it possible to reduce significantly the time and effort required to publish legislative information electronically. When fully implemented, the technology promises to provide immediate access to newly created legislative information from the authoritative source for that information. The House Oversight Committee's report, "An Information Systems Program Plan for the U.S. House of Representatives," led

---

[30] William Jackson, "Technology Report: Video on Demand, *Government Computer News*, October, 21, 2002, p.29-30.

[31]Tom Davis, Chairman, Committee on Government Reform, Adam Putnam, Chairman, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, *Joint Statement on Electronically Databasing Committee Hearings with Text Searchable Applications,* March 13, 2002 [http://www.house.gov/reform/davis_putnam.pdf].

[32] Congress Online Project, *E-mail Overload in Congress: Managing a Communications Crisis,* March 2001, [http://www.congressonlineproject/email.html].

[33] Amy Keller, "Anthrax Fears Boost Importance of E-mail on Hill," *Roll Call*, October 25, 2001, p. 1; and Preeti Vasishtha, "House Sees E-mail Spike," *Government Computer News*, November 5, 2001, p.1.

[34]Congress Online Project, *Congress Online: Special Report E-mail Overload in Congress - Update*, August 7, 2002, [http://www.congressonlineproject/pf080702.html].

[35]Ibid.

to the clerk's proposal to create a comprehensive system for print-on-demand capabilities and improvements to electronic information flow in the House.[36]

A component of the House DMS project is the establishment of a standards-based program for the exchange of information between legislative branch organizations that will, over time, significantly improve IT planning and implementation. In the 106th Congress, the Committee on House Administration initiated the effort to develop such a standards-based program with a review of the way in which legislative and various other House information was created and managed. The committee directed the Clerk of the House to establish data standards for legislative information, and, in July 1999, directed the Clerk to initiate a feasibility study in collaboration with staff from the House, Senate, GPO, LOC, and CRS. The study was completed in 2000, and recommended the deployment of an Extensible Markup Language (XML)-based[37] authoring system for bills and resolutions. Currently in the initial stages of implementation, the House of Representatives uses the system for the production of simple resolutions.[38]

The Integration of Emergency Communications. In the aftermath of the attacks on the United States on September 11, 2001, the Committee on House Administration issued a BlackBerry, a wireless personal digital assistant (PDA), charging station and other accessories to each Representative. The committee also provided user training for the devices. The purpose of the BlackBerry is to communicate critical information to Members when other modes of communication may be inoperative. The BlackBerry can be used as a pager or e-mail device, and the House is investigating the possibility of extending the capabilities of the PDA to include Web browsing.[39]

---

[36] See U.S. Congress, House, Committee on House Oversight, *Report on the Activities of the House of Representatives during the One Hundred Fifth Congress Together with Minority and Additional Views*, House Report 105-850, 105th Congress, 2nd session, (Washington: GPO, January 2, 1999), p. 20. Parts of the report, "An Information Systems Program Plan for the U.S. House of Representatives," can be found in CyberCongress Accomplishments During the 104th Congress.

[37] XML is designed especially for Web documents, and allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.

[38] See Susan M. Menke, "House Resolutions in XML," *Government Computer News*, July 2, 2002 at [http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcndaily2&story.id=19207]; and "House Builds and XML Foundation," *Government Computer News*, August 27, 2001 at [http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcn2&story.id=16922].

[39] 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, October 16, 2000. [http://www.house.gov/cha/publications/DC_s/dc_s.html]. Ephraim Schwartz, "Congress Going Wireless," InfoWorld, October 12, 2001, at [http://www.nwfusion.com/net.worker/news/2001/1012conwless.html].

Use of Electronic Devices on the Floor. While some IT systems have been integrated into House floor operations for many years,[40] none of these systems is available for individual Representatives' use. House rules have long forbidden the use of pagers, personal digital assistants, wireless telephones, and other electronic devices by Members on the floor. At the beginning of the 108th Congress, Rule XVII, clause 5 was amended to forbid only "a wireless telephone or personal computer." in the new Congress. According to the summary submitted by the chair of the Rules Committee, unobtrusive handheld electronic devices, will be permitted on the floor.[41] A BlackBerry is an example of such a device.

Information Technology Oversight, 108th Congress. In the 108th Congress, the Committee on House Administration has announced several initiatives related to the oversight and management of House IT activities. According to the committee's oversight plan, the committee will continue to oversee the operations of House Information Resources and other technology functions of the House. Other oversight activities will likely include monitoring the implementation of House Rule XI 2(e)(4) requiring committee documentation to be made available electronically, reviewing computer security measures in the House, and overseeing implementation of the committee hearing room upgrade program. Working with the Senate, the committee anticipates overseeing forums for the sharing of technology plans and capabilities among the legislative branch agencies, and continuing improvements to the Legislative Information System.[42]

Public Access

A significant component of the House of Representatives IT integration strategy has been to enhance public access to information about congressional activity. This includes documents, information about Members and House officers, and remote access to House proceedings. Public access initiatives have included THOMAS, and the development of a House-wide Web page, as well as broad- and narrowcasting of House floor and committee proceedings.

THOMAS. One of the earliest efforts to provide public access to materials documenting congressional activity was the introduction of THOMAS [http://thomas.loc.gov/], available through the Library of Congress. Named in honor of Thomas Jefferson, the service went online in January 1995. THOMAS was the first comprehensive electronic legislative information system distributing House and Senate information to the public via the Internet. From its inception, the system has provided the full text of bills from both chambers, accessible by keyword and bill

---

[40] A limited number of hard-wired telephones are used in the chamber, along with electronic voting stations, and computers and other electronic equipment at the respective floor managers' tables, employed to monitor the progress of votes.

[41] Section-By-Section Summary of H.Res. 5, inserted material, *Congressional Record*, daily edition, vol. 149 (Jan. 7, 2003), p. H12 (also available at [http://www.house.gov/rules/108rules_secsum.htm]); also, see announcement by the Speaker that day about electronic devices, Ibid., p. H23.

[42] *Committee on House Administration 108th Congress Oversight Plan*, undated, available on the Web at [http://www.house.gov/cha/noversight.htm].

number. Shortly thereafter, the *Congressional Record* text and index and legislative status information were added. Later enhancements to THOMAS included links to House and Senate voting files, committee reports, and selected hearing transcripts, as well as improved search and display capabilities.

House Public Web Sites. Concurrent with the debut of THOMAS, the House Oversight Committee launched a Web site for the House [http://www.house.gov/] providing public access to information about Members of Congress, committees, and organizations of the House of Representatives and to other U.S. government information resources. By the end of the 104th Congress, 222 Members of Congress, 27 committees, and 11 other House offices had launched Web sites on the House Web server.

Currently, all Members and committees maintain a Web presence. A recent report by the Congress Online Project suggests that the Web sites maintained by Member and leadership offices offers a wide array of content, in some cases functioning as a virtual office for constituents to visit online. According to the report, the Web offers the Members and leadership of the House the opportunity to take advantage of emerging technologies as a tool of communication with constituents, media and other interested parties.[43]

Broadcast and Narrowcast. Audio and video capabilities in the House of Representatives also play a major role in public access to Congress. Television coverage of the floor proceedings has existed for many years, along with C-SPAN coverage of selected hearings. Members of Congress make routine use of video technology designed to deliver a custom message to a narrow audience, such as a specific group of constituents, and to provide material for the news media. Video conferencing technology is now available in a growing number of House offices, as well as centrally through the House recording studio. An advance in this area is audio and video distribution over the Internet. The potential use of these technologies for Congress continues to expand along with technological innovation.

Information Technology Issues and Options in the House of Representatives

The more routine integration of technology into Member and committee operations, and the heightened prominence of homeland security concerns has also signified a transition in House IT issues. While the technology environment continues to evolve, requiring the introduction of new initiatives, more attention is being focused on the sustainability of projects and the recruitment and retention of skilled IT human capital. There has also been a significant emphasis on issues related to emergency communications and continuity of operations (COOP) planning.

---

[43] Congress Online Project, *Congress Online 2003: Turning the Corner on the Information Age*, at [http://www.congressonlineproject.org/webstudy2003.html].

Considerations of the use of IT often focus on the technology itself, rather than the purpose to which the technology is being applied. To a limited extent, technical considerations can be helpful in evaluating issues related to logistics, costs, convenience, usability, and environmental factors, such as noise or accommodating new supporting infrastructure in House facilities. These factors may be important in determining what systems or devices may be accommodated in specific locations, whether adjustments need to be made to adopt a technology, or which technologies appear preferable from the user's perspective. Other factors, such as whether Members of Congress and staff are comfortable using those technologies, whether products meet designated requirements, and how well they fit into the culture of the institution, are also critical to their acceptance. Some emerging and ongoing IT issues that are confronting the House of Representatives, and some potential approaches for responding to them are discussed below.

Emerging Issues

House Continuity of Operations (COOP) Planning. 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 planning for the continuity of government (COG). COG planning focuses on ensuring the government's ability to continue its minimum essential responsibilities (the critical subset of responsibilities that would be covered by a COOP plan) while assuring the survival of a country's constitutional and representative form of government in the event of a catastrophic emergency.[44]

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).[45] Responsibility for securing and backing up committee and Member hard

---

[44]For more information regarding COG, see CRS Report RS21089, *Continuity of Government: Current Federal Arrangements and the Future*, by Harold C. Relyea.

[45]The House legislative information management system contains the metadata(or data about 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

(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 has maintained a longstanding plan to relocate floor activities in the event that Capitol facilities are unavailable. 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.

Emergency Communications Sustainability. Although technology-based communications are becoming more common, it is not clear how robust they would be under emergency circumstances. A natural disaster, intentional physical damage, software failure, or cyberattack on telecommunications networks might degrade or interrupt voice, teleconference, and videoconference capabilities. A surge in demand on these networks at the time of the event might also impair their effectiveness. This was demonstrated in New York and Washington, DC on September 11, 2001, when wired and wireless voice telecommunications were significantly hampered due to attack related damage to the networks and extraordinary demand by users.[46]

Although Congress has adopted many other communications technologies, it does not appear to have adopted a secure, wide ranging remote emergency communications system capable of enabling Members to communicate their whereabouts and availability, or receive instructions in the event of an operational interruption or other unforeseen contingency. An example of the challenges of using networks designed to carry routine communications as emergency systems can be found in the limited, non-secure communications system accessed through a BlackBerry portable digital assistant (PDA) issued to each Representative. When Members are in Washington, DC, this system could be used to provide Members with critical information during an emergency, assuming that the network that supports the devices stays online throughout the event. If an incident occurred when Congress was not in session, however, the devices could be of limited use because

---

[45](...continued)
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].

[46]See Megan Lisagor, "Reinventing FEMA," *Federal Computer Week*, March 25, 2002, at [http://www.fcw.com/fcw/articles/2002/0325/cov-fema-03-25-02.asp]. Also, see CRS Report RL31542, *Homeland Security – Reducing the Vulnerability of Public and Private Information Infrastructures to Terrorism: An Overview*, by Jeffrey W. Seifert, pp. 2-4.

the network does not serve every state in the Union.[47] The utility of the BlackBerry devices might be further reduced due to concerns regarding the ability to authenticate users as the Members themselves. Congress might wish to consider potential approaches to ensure its capacity to communicate and carry out its constitutional responsibilities in a time of crisis.

Digitized Mail. Under the direction of the Committee on House Administration, the CAO has invited proposals from vendors to open, scan and digitize first-class and flat postal mail for digital delivery. Observers note that a digitized system would reduce the delay due to steps currently used to safeguard congressional mail, by providing electronic images of mail before the original paper copies have completed decontamination and inspection procedures. Other observers raise concerns that allowing outside vendors to process congressional mail may compromise the privacy of constituents and others who write to Members of Congress and delay the process for ordering and paying for flags flown over the Capitol. Under the proposed scanning program, checks and other financial instruments would not be scanned, but would be forwarded to the appropriate office after decontamination and inspection procedures have been completed. The successful bidder will initially implement a pilot program of 50 House Members and two committees before expanding operations to serve all House of Representatives offices. The pilot program is expected to be initiated by the end of August, 2002.[48]

Electronic Congress (e-Congress).[49] Some observers have offered broad suggestions involving the establishment of a Web site that Members of Congress could access from any location beyond the Capitol complex. It has been suggested that such a Web site could enable Members of Congress to carry out activities normally done on the chambers' floors or in committees. These suggestions generally highlight the use of information technology (IT) to enable Congress to carry out its responsibilities remotely, as a substitute for traditional congressional functions performed in Washington. These proposals tend to focus on floor activity while not systematically addressing other areas of congressional activities, such as committee business[50] and Member office operations. In addition to these matters, the possibility

---

[47] According to Cingular, the BlackBerry network provider for the House of Representatives, "the Cingular Intelligent Wireless Network covers approximately 93% of the U.S. business population." The network provides only limited service in some states and no coverage in several others. See [http://www.earthlink.net/mobile/blackberry/coverage/]. Network coverage is also discussed at [http://www.blackberryme.com/950957network.html].

[48] David Enrich, "House to Try Scanned-In Letters," *The Washington Post*, July 8, 2002, p. A15; and Dan Davidson and Chet Dembeck, "House Bids to Convert Mail to E-mail," *Federal Times*, Vol. 39 No 1, June 24, 2002, p. 1.

[49] For more information regarding on the potential development of an electronic Congress, see CRS Report RS21140, *Electronic Congress: Proposals and Issues*, by Jeffrey W. Seifert and R. Eric Petersen.

[50] A preliminary proposal for the creation of "virtual" hearing room was recently offered. Representative Curt Weldon has suggested that the creation of a facility equipped with secure workstations and videoconferencing technology could enable committee members in Washington, DC to question witnesses at remote locations. See Dan Caterinicchia,

(continued...)

of convening an e-Congress raises a number of procedural, technical, and resource questions, including concerns regarding deliberation, information security, and costs.

Ongoing Issues

IT Staffing. As IT systems grow more complex and if they are more intensively relied upon to carry out congressional operations, it may be necessary for lawmakers to determine how best to manage those systems in congressional offices. Currently, some House committees and a few Member offices employ full-time, dedicated information systems administrators to manage advanced technology systems. Other offices assign staff to oversee this work on a part-time basis, along with a range of other duties. In light of recent changes to House regulations, a third option used by some offices includes contracting with outside companies to create and maintain Member Web pages.[51] These developments lead to considerations about the possible need for dedicated IT staff, potential impediments to recruiting and retaining IT specialists, or contract management and oversight, as well as the effect of dedicated systems administration on other congressional office operations in the House of Representatives.

Legislative Document Authentication. The use of IT to automate the preparation of legislative documents, combined with increasing use of networks for exchanging text and distributing documents, has increased the speed and process of preparing bills, committee reports, and other legislative documents. An effective document management system makes document preparation more efficient. Documents that originate in digital form do not have to be converted or re-keyed, reducing the time needed for publication and enhancing the options for electronic distribution. The use of common formatting standards also contributes to the improvement of both the print and electronic publication processes. Offices in the House, Senate, LOC, and GPO that are involved in the preparation and publication of legislative documents have developed a common set of Standard Generalized Markup Language (SGML)[52] "tags"[53] to describe the core components of legislative material. Using this common set of tags facilitates the printing process and establishes a standardized format for documents used throughout the legislative process.

---

[50](...continued)
"Weldon Envisions Virtual Hearings," *Federal Computer Week*, May 27, 2002, p. 12.

[51]William Matthews, "Hill Calls on Web Experts," *Federal Computer Week*, June 11, 2001, p.26.

[52]SGML is a system for organizing and tagging elements of a document. SGML was developed and standardized by the International Organization for Standards (ISO) in 1986. SGML itself does not specify any particular formatting; rather, it specifies the rules for tagging elements. These tags can then be interpreted to format elements in different ways.

[53]Tags are identifiers, or computer instructions, inserted in a document that specifies how subsequent portions of the document, should be formatted. For example, in a document, a tag could be used to identify a bill's sponsor while another tag would identify where the measure is in the legislative process.

The ongoing transition to a more comprehensive electronic environment raises several issues. It is not clear, for example, what constitutes a "document" in an environment where paper and electronic versions are available in a variety of formats. The integration of clickable Web links also raise concerns about the authenticity and reliability of some documents. Combining these linked pieces of information, which may originate from several sources both inside and outside the House of Representatives, may be essential to conveying a complete message. Thus far, it is not clear in this context whether collections of linked Web pages are considered documents for use in the activities of the House of Representatives.

If they are documents, there may also be concerns about how the information in those documents will be maintained. In some cases, the House of Representatives may not have complete control over documents which circulate electronically because they contain information from databases beyond the control of the chamber.

Another element of complexity may be added by potentially integrating the video recording of House of Representatives floor proceedings with the text to provide for a multimedia version of the *Congressional Record*. Similarly, as committees publish more of their hearings and mark-up information on the Internet, and release video coverage of their proceedings, they may be faced with similar questions.[54]

Closely linked with the use of multiple information formats is the issue of determining what is considered the "official" version of congressional materials and whether online publication satisfies current chamber rules requiring the retention of House of Representatives records.[55] Ascertaining the authenticity and status of the various versions may be an increasingly important use of electronic versions of the *Congressional Record* and other legislative materials. Within a day, there are three versions of the floor proceedings available—the daily printed version of the *Congressional Record*, the online version, and the video version.[56] House rules allow Representatives subsequently to amend and extend their remarks in the *Congressional Record* and correct any errors that exist in the text. A second, corrected version of the proceedings is produced when GPO prints the permanent

---

[54]Rule XI clause e(4) requires each committee to "...make its publications available in electronic form to the maximum extent feasible." See U.S. Congress, House, *House Rules and Manual, 107th Congress*, p.796.

[55]Rule VII clause (6) define the term 'record' as "... any permanent official record of the House (other than a record of an individual Member, Delegate, or Resident Commissioner)..." but it does not define the format of those records.

[56]No official index is kept of video recordings of proceedings. The official video archive of House floor proceedings is maintained by the Motion Picture and Video Branch of the National Archives. The Library of Congress maintains the same collection for public use. Retrieval of video from these sources is based on the details of floor proceeding presented in the *Congressional Record*. Each archive contains video proceedings of all House floor activity since cameras were allowed in the chamber in 1979. An unofficial, partially indexed video archive of House floor proceedings is maintained by C-SPAN. These materials, which include House of Representatives floor proceedings from 1987 to the present, and may be accessed at [http://www.pava.purdue.edu/].

bound version of the *Congressional Record*. The final bound version is considered the official version, but is generally not printed for several years after House of Representative proceedings have occurred.

In contrast, it is possible to make speedy corrections to the online version of the *Congressional Record* that give it the appearance of being "final." Yet, the appearance of a correctly formatted document may mask the fact that there has been little time to analyze or validate the content. The ability to "cut and paste" text from one document to another might improve the consistency of legislation over time, but also could result in increasingly lengthy documents. Also, given the broad public access to the *Congressional Record* over the Internet, the need to make available an official version quickly becomes more critical. On the other hand, as external composition is forced to accelerate under this process, one loses the time between each stage that historically has been available for further consideration of wording and quality control. This issue will likely be a topic of discussion as it continues to evolve. The printed version is generally considered the official version, although it is the certification by the Clerk of the House that actually makes the document official.

Security and Authentication. Implementation of new technologies will depend on their reliability and security. Increasing reliance on IT systems raises questions about the trustworthiness of these technologies and the potential dependency of an institution such as the House of Representatives on systems that may fail to operate as and when needed. The requirements for adequate safeguards against unauthorized access and misuse of House systems present ongoing challenges to be addressed before new systems and capabilities are implemented.

Related to questions of IT management and security is the transparency of information management. In this context, transparency refers to the ability to accurately trace and verify the source of the information being used to create online databases and electronic documents. Issues of concern for policymakers in this area include the sources and control of information. The acceptance of electronic documents as policy instruments will be heavily dependent on their perceived authenticity and reliability. To achieve these qualities, characteristics such as their source, author, and version must be clearly established and verified. In addition to contributing to the legitimacy of online information, transparency is also related to concerns of trust in IT. Trust, as it relates to IT, usually refers to one's confidence in the reliability and dependability of the physical infrastructure. This is an important concern when considering a shift to a more technologically enhanced and dependent environment, such as movement toward electronic government.

An issue related to document authentication is the use of electronic signatures.[57] An electronic signature is a code that is attached to a digitally transmitted message or document that uniquely identifies the sender. The purpose of an electronic signature is to guarantee the authenticity of the sender. Electronic signatures are

---

[57]See CRS Report RS20344, *Electronic Signatures: Technology Developments and Legislative Issues*, by Richard M. Nunno, for a more comprehensive analysis of legislative issues related to electronic signatures.

currently not in use in the House of Representatives. Electronic signature technology has the potential to allow Members of Congress to carry out some responsibilities electronically that they currently do in person or in written form. However, the potential use of electronic signatures may conflict with some assumptions regarding Members' actions and delegation of authority. Issues of author authentication include:

- whether current rules governing requirements for Representative's signatures could apply to electronic documents;
- who will have authority to use an electronic signature, or under what circumstances a Representative would need to actually sign documents; and
- whether staff may use an electronic signature on behalf of a Member of Congress in a manner similar to employing a signature machine or signing for the Representative.

Trust is also important to convince users of the integrity of the information upon which they rely. Documents that have been submitted through the appropriate channels to be printed ultimately by GPO or other sanctioned printers carry an imprimatur of legitimacy that other electronic formats from other sources do not necessarily have. The Chief Administrative Officer of the House of Representatives recently conducted technical evaluations of electronic signature systems and other electronic authentication methods, including biometrics.

Managing E-mail. As e-mail has become a more typical means of communication, the relatively high volume of electronic messages sent to the House has highlighted differences in perceptions of e-mail, and how it is handled, between congressional constituent communications and citizen or customer communications with other public or private sector entities. First, the decentralized nature of the House of Representatives means that every Member's office attends to its e-mail needs separately, compared to federal agencies or corporations which often have centralized offices for handling technical and resource requirements.[58] A second difference is that, while private sector entities may view e-mail as a cost-savings measure, it is a mixed blessing for the House of Representatives. Congressional concerns about security, including message tampering, and identifying constituents from non-constituents, are obstacles to implementing automated e-mail response systems and a broader shift to routine two way electronic communications. A third difference is the perceived importance of e-mail. While many constituents view their e-mail messages to Congress as being as important as phone calls or postal mail, many congressional offices do not share this view and assign a lower priority to responding to e-mail messages.[59] These concerns have been exacerbated by the use

---

[58] Congress Online Project, *E-mail Overload in Congress*, [http://www.congressonlineproject/email.html].

[59] David McGuire, "Lawmakers still Prefer Snail Mail," The Washington Post, May 8, 2002, [http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A53591-2002May8]; and Rebecca Fairley Raney, "E-mail Finds the Rare Ear in Congress,"

(continued...)

of unsolicited commercial e-mail (spam[60]) by interest groups, which accounts for a significant portion of the volume of e-mail. Should the volume of messages significantly grow, some observers suggest that the House of Representatives may wish to consider additional refinements to its coordinated technical approach to managing the flow of e-mail messages, to maintain current service levels and decrease the vulnerability of its systems to collapse by sudden, sharp increases in message volume.

The Deliberative Process. The impact of electronic devices on the deliberative process of the House of Representatives is of concern. Some observers fear that the transition to an electronic document system may have the effect of reducing time for deliberation throughout the legislative process. The use of computers makes it possible to present draft material in a format that appears to be final and complete. Yet, the appearance of a correctly formatted document may mask the fact that there has been little time to discuss, analyze, or validate the content. As legislative text moves more seamlessly from initial drafts through final publication, one may potentially lose the time between each stage of the process that historically has been available for further consideration of the wording, for performing quality control, and for informal deliberation. Decisions on integration of IT in the House of Representatives will likely be influenced by these factors.

Document Publication and Distribution. As demand for immediate access to information increases and the costs to print information on-demand in a distributed manner continues to decline, the relative advantages of electronic systems vis-à-vis the centralized printing by GPO become a subject of debate. Some observers argue that central control provides the greatest assurance that official government documents will be available to the public.[61] Others maintain that the changing technologies—both for printing and for making documents accessible online—offer greater efficiencies and broader opportunities for public access.[62]

Archiving Information. Another issue that is rapidly growing government-wide is the creation and maintenance of electronic information archives. The proliferation of various text, audio, and video media formats, and the uneven use of Web sites, e-mail, and other means of communications, create many challenges to

---

[59](...continued)
The New York Times, December 13, 2001, p. G11. Also, see Congress Online Project, *E-mail Overload in Congress*, [http://www.congressonlineproject/email.html].

[60]See CRS Report RS20037, *"Junk E-mail": An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam")*, by Marcia S. Smith for a more comprehensive analysis of the issues related to spam.

[61] These arguments are discussed in CRS Report 98-687, *Public Printing Reform: Issues and Actions*, by Harold C. Relyea, pp. 1-10.

[62] Office of the Vice President (Gore), *From Red Tape to Results: Creating a Government That Works Better and Costs Less, Report of the National Performance Review* (Washington: GPO, 1993), p. 5-8. Other similar views are summarized in U.S. General Accounting Office, *Government Printing Office: Monopoly-Like Status Contributes to Inefficiency and Ineffectiveness*, GAO Report GAO/GGD-90-107 (Washington: September 1990).

maintaining the public record. In Congress, some committees and individual Representatives extensively utilize electronic resources to communicate with their respective constituencies. Some committees stream live audio and video feeds of hearings over the Internet and post documents that can be downloaded. Although some Members of Congress make active use of e-mail and Web sites to respond to inquiries, other Members rely on more traditional paper-based means of providing information to produce written letters and press releases. The House has not yet addressed the issue of archiving congressional digital audio and video resources at a level comparable to that of paper-based records.[63]

During transitions, Web sites may be closed down or significantly changed. In the executive branch, the National Archives attempted to preserve executive branch Web sites during the recent change of administrations.[64] Some observers suggest the House of Representatives may wish to consider undertaking end-of-service or end-of-term reviews as membership changes and as the content of House Web sites is updated.

Information Access and Continuity. Related to the electronic publication and archiving of documents are issues regarding long term access to them. Among the issues involved are matters of how to keep track of what information is made available to the public electronically, and the decision process to determine what information should be archived, and how to make it available to the public. An additional consideration is what happens when electronic formats become obsolete and potentially unreadable and whether it will become necessary to convert electronic information continually to new formats as the technology develops. Addressing these issues and questions of maintaining the long-term accessibility and preservation of electronic congressional records will fall to committees, the Office of the Clerk, the House Librarian, the LOC, and GPO.

E-Government.[65] As the above issues suggest, the growth of the use of IT generates opportunities, challenges, and concerns for the House of Representatives, as it does for executive agencies seeking to streamline government processes and enhance efficiency. However, unlike executive branch agencies, the less quantifiable, deliberative nature of the legislative process likely will strongly influence the kinds of goals and efficiency measures of interest to the House of Representatives. The House of Representatives may choose to look to the state legislatures as examples for practices that support the distinctive objectives of legislative institutions.

---

[63]Source: Discussions with staff from the Committee on House Administration.

[64]For information on government printing issues see CRS Report RL30590, *Paperwork Reduction Act Reauthorization and Government Information Management Issues*, by Harold C. Relyea; and CRS Report 98-687, *Public Printing Reform: Issues and Actions*, by Harold C. Relyea.

[65]For a broader discussion of e-government concepts and issues, see CRS Report RL30745, *Electronic Government: A Conceptual Overview*, by Harold C. Relyea, CRS Report RL31088, *Electronic Government: Major Proposals and Initiatives*, by Harold C. Relyea, and CRS Report RL31057, *A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance*, by Jeffrey W. Seifert.

Selected Glossary of Information Technology and E-Government Terms[66]

architecture - usually refers to the overall structure of computers, networks, and other IT products and systems, in terms of the hardware and/or software that compose the product. By comparison, the term "design" connotes thinking that has less scope than architecture. An architecture is a design, but most designs are not architectures. A single component or a new function has a design that has to fit within the overall architecture.

call center - a central place where customer and other telephone calls are handled by an organization, usually with some amount of computer automation. Typically, a call center has the ability to handle a considerable volume of calls at the same time, to screen calls and forward them to someone qualified to handle them, and to log calls. Call centers are used by computer product help desks, mail-order catalog organizations, telemarketing companies, and any large organization that uses the telephone to sell or service products and services.

CapNET - the Capitol Hill wide area network that links together the various legislative branch computer systems.

connectivity - a program or the ability of a device to link with other programs and devices. For example, a program that can import data from a wide variety of other programs and can export data in many different formats is said to have good connectivity. On the other hand, computers that have difficulty linking into a network (many laptop computers, for example) have poor connectivity.

cookies - small text files placed on a user's computer by a web server so that it can track the user's movement through a Web site. Originally designed to allow user-side customization of Web information, the expanded use of cookies has raised concerns about the privacy of a user's Web browsing activities.

digital subscriber line (DSL) - a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. For homes or small businesses close enough to a telephone company central office that offers DSL service, one may be able to receive data at rates up to 6.1 megabits (millions of bits) per second, enabling continuous transmission of motion video, audio, and even 3-D effects. More typically, individual connections will provide from 1.544 Mbps to 512 Kbps downstream (downloading from the Internet to a computer) and about 128 Kbps upstream (uploading or sending information from a computer through the Internet). A DSL line can carry both data and voice signals and the data part of the line is continuously connected. DSL installations began in 1998

---

[66] This glossary is based on definitions found in various online IT dictionaries, including *ISP Glossary* at [http://isp.webopedia.com/]; *Webopedia* at [http://www.webopedia.com/]; National Committee for Information Technology Standards Information Technology Dictionary at [http://www.ncits.org/tc_home/k5htm/ANSDIT.htm]; and *Whatis.com* at [http://whatis.techtarget.com/].

and will continue at a greatly increased pace through the next decade in a number of communities in the U.S. and elsewhere. DSL is expected to replace ISDN in many areas and to compete with the cable modem in bringing multimedia and 3-D to homes and small businesses.

electronic signature - a code that is attached to a digitally transmitted message or document that uniquely identifies the sender. The purpose of an electronic signature is to guarantee the authenticity of the sender.

encryption - the translation of data into a form of secret code called ciphertext. To read an encrypted file, one must have access to a secret key or password that enables the user to decrypt it. Unencrypted data is called plain text.

enterprise - often used in the computer industry to describe any large organizations, including corporations, small businesses, non-profit institutions, or government bodies, that utilize computers. In practice, the term is applied much more often to larger organizations than smaller ones. An intranet is an example of an enterprise computing system.

extensible markup language (XML) - a specification developed by the World Wide Web Consortium, an international consortium of companies involved with the Internet and the Web. XML is a pared-down version of SGML, designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.

firewall - a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

hypertext transfer protocol (HTTP) - the underlying application protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

hyperlink - an element in an electronic document that links to another place in the same document or to an entirely different document. Typically, one clicks on the hyperlink to follow the link.

hypertext - the organization of information units into connected associations, using hyperlinks, that a user can choose to make. Information units can include, but are not limited to, text, pictures, music, and programs. For example, while reading a document about Mozart, one might click on the phrase Violin Concerto in A Major, which could display the written score or perhaps even invoke a recording of the

concerto. Hypertext was the main concept that led to the invention of the World Wide Web, which is the product of an ever-growing amount of information content connected by an ever-growing number of hypertext links.

infrastructure - in reference to IT and the Internet, the physical hardware used to interconnect computers and users. Infrastructure includes the transmission media, including telephone lines, cable television lines, and satellites and antennas, and also the router, aggregator, repeater, and other devices that control transmission paths. Infrastructure also includes the software used to send, receive, and manage the signals that are transmitted.

integrated service digital network (ISDN) - an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires. ISDN supports data transfer rates of 64 Kbps (64,000 bits per second). Most ISDN lines offered by telephone companies provide two lines at once, called B channels. One line may be used for voice and the other for data, or both lines for may be used for data to produce data rates of 128 Kbps, three times the data rate provided by today's fastest modems.

intranet - a network based on TCP/IP protocols belonging to an organization, such as a corporation or agency, that is accessible only by the organization's members, employees, or others with authorization. In essence, an intranet functions like an internal Internet that is not accessible to the general public.

kilobits (kb) - 1,024 bits for technical purposes, such as data storage; 1,000 bits for general purposes. Data transfer rates are measured in kilobits per second, abbreviated as Kbps, and count a kilo as 1,000 bits.

laptop - frequently called notebook computers, laptop computers are small, battery-powered, portable computers. A laptop typically weighs less than 5 pounds and is 3 inches or less in thickness.

Legislative Information System (LIS) - a Web-based system designed to provide Members of Congress and their staff with access to the most current and comprehensive legislative information available. Some of the information in LIS includes the text of bills, the *Congressional Record,* and committee reports. It is available only to the House, Senate and legislative support agencies.

link - see hyperlink

local area network (LAN) - a group of computers and associated devices (computer network) that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. Users can also share devices such as laser printers. A local area network may serve as few as two or three users (for example, in a home network) or many thousands of users.

narrowcast - to send data to a specific list of recipients. Cable television is an example of narrowcasting since the cable TV signals are sent only to homes that have

subscribed to the cable service. In contrast, network TV uses a broadcast model in which the signals are transmitted everywhere, and anyone with an antenna can receive them.

network - a group of two or more computers linked together. Networks can interconnect with other networks and contain subnetworks.

operating system - a program that runs on a computer to provide a software platform on top of which other programs, called application programs, can run. Every general purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers. The choice of operating system determines to a great extent the applications that can be run. For PCs, some of the most popular operating systems are DOS, Windows, and Linux.

portal - a Web site or service that serves as a central resource for information and services, such as e-mail, discussion forums, search engines, and online shopping.

server - a computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries.

standard generalized markup language (SGML) – a system for organizing and tagging elements of a document. SGML was developed and standardized by the International Organization for Standards (ISO) in 1986. SGML itself does not specify any particular formatting; rather, it specifies the rules for tagging elements. These tags can then be interpreted to format elements in different ways. SGML is used widely to manage large documents that are subject to frequent revisions and need to be printed in different formats. Because it is a large and complex system, it is not yet widely used on personal computers.

TCP/IP (Transmission Control Protocol/Internet Protocol) - is the suite of communications protocols used to connect computers on the Internet. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks.

THOMAS - a Web-based federal legislative information system made freely available to the Internet public. Thomas was created by a Library of Congress team, under the direction of the leadership of the 104th Congress, and was brought online in January 1995, at the inception of the 104th Congress. [http://thomas.loc.gov/]

transparency - in the context of information management, the ability to trace accurately and verify the source of the information being used to create online databases and electronic documents. Issues of concern in this area include the sources and control of information.

virtual private network - a network that is constructed by using public networks, such as the Internet, to connect computers for exchanging data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

virus - a program or piece of code that becomes loaded onto a computer without the user's knowledge and runs against one's wishes. Viruses can be transmitted by sending them as attachments to an e-mail note, by downloading infected programming from other sites, or be present on a diskette or CD. Most viruses can replicate themselves. All computer viruses are created by humans. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances (such as the passing of a date or time) cause their code to be executed by the computer. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. A virus is not the same as a worm, but some newer viruses are a hybrid of the two types of programs.

worm - a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs and does not alter files. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

XML - See extensible markup language.

For Additional Reading

House Documents

Bob Ney, Chairman, Committee on House Administration, *New Computer Anti-Virus Protection for the House*, Dear Colleague Letter, January 23, 2001. [http://www.house.gov/cha/publications/publications.html].

Bill Thomas, Chairman, Committee on House Administration, *Reinforcing Security of Office Servers*, Dear Colleague Letter, June 20, 2000. [http://www.house.gov/cha/publications/publications.html].

U.S. Congress, House, *House Smart: House Reference Guide to Information and Services*, 108th Congress, 1st session (Washington, 2001)

U.S. Congress, House Committee on House Administration, *106th Congress Oversight Plan*. [http://www.house.gov/cha/oversightplan106th.htm].

U.S. Congress, House, Committee on House Administration, "The United States House of Representatives General Information Security Guidelines for Protecting Systems from Unauthorized Use," HISPOL 002.0, Issued, February

4, 1998, revised, October 17, 2000. [http://onlinecao.house.gov/hir-security/hisdoc.htm].

U.S. Congress, House, Committee on House Administration, "Protection for Member and Committee Office Systems from Unauthorized Use," HISPOL 002.1. [http://onlinecao.house.gov/hir-security/hisdoc.htm]

U.S. Congress, House, Committee on House Administration, "Internet/Intranet Security Policy," HISPOL 003.0. [http://onlinecao.house.gov/hir-security/hisdoc.htm]

U.S. Congress, House, Committee on House Administration, "Information Security Policy for Information System-Related Security Incidents," HISPOL 004.0. [http://onlinecao.house.gov/hir-security/hisdoc.htm]

U.S. Congress, House, Committee on House Administration, "Information Security Policy for Vendor Remote Access to the House Network," HISPOL 005.0. [http://onlinecao.house.gov/hir-security/hisdoc.htm]

U.S. Congress, House, Committee on House Oversight, *Report on the Activities of the House of Representatives during the One Hundred Fifth Congress Together with Minority and Additional Views*, House Report 105-850, 105th Congress, 2nd session, (Washington: GPO, January 2, 1999)

U.S. Congress, House Committee on House Oversight, *CyberCongress Accomplishments During the 104th Congress.* Presented by the Computer and Information Services Working Group to the Committee on House Oversight, February 11, 1997.

U.S. Congress, House, Committee on House Oversight, *Report on the Activities of the Committee on House Oversight of the House of Representatives During the One Hundred Fourth Congress*, House Report 104-885, 104th Congress, 2nd session, (Washington: GPO, January 2, 1997)

U.S. Congress, House, Office of Inspector General, *Audit Report: House Computer Systems Were Vulnerable to Unauthorized Access, Modification, and Destruction*, Report No. 95-CAO-18, July 18,1995. [http://www.house.gov/IG/page2.htm].

U.S. Congress, House, Office of Inspector General, *Audit Report: The Management and Control of the House's Information Systems Operations Should be Improved to Better Meet Member's Needs*, Report No. 95-CAO-19, July 18,1995. [http://www.house.gov/IG/page2.htm].

U.S. Congress, House, Office of Inspector General, *Audit Report: The House Needs to Follow a Structured Approach for Managing and Controlling System Development Life Cycle Activities of its Computer Systems*, Report No. 95-CAO-20, July 18,1995. [http://www.house.gov/IG/page2.htm].

CRS Products

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

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

CRS Report RL30745. *Electronic Government: A Conceptual Overview*, by Harold C. Relyea

CRS Report RL31088. *Electronic Government: Major Proposals and Initiatives*, by Harold C. Relyea

CRS Report RS20344. *Electronic Signatures: Technology Developments and Legislative Issues*, by Richard M. Nunno

CRS Report RL30914. *Federal Chief Information Officer (CIO): Opportunities and Challenges*, by Jeffrey W. Seifert

CRS Report RL30661. *Government Information Technology Management: Past and Future Issues (The Clinger-Cohen Act)*, by Jeffrey W. Seifert

CRS Report 98-67. *Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth*, by Marcia S. Smith, John D. Moteff, Lennard G. Kruger, Glenn J. McLoughlin, and Jeffrey W. Seifert.

CRS Report RL30784 *Internet Privacy: An Analysis of Technology and Policy Issues*, by Marcia S. Smith.

CRS Report RS20037 *Junk E-mail: An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam")*, by Marcia S. Smith

CRS Report RL30590. *Paperwork Reduction Act Reauthorization and Government Information Management Issues*, by Harold C. Relyea

CRS Report RL31057. *A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance*, by Jeffrey W. Seifert

CRS Report 98-687. *Public Printing Reform: Issues and Actions*, by Harold C. Relyea.

Other Resources

Chris Casey, *The Hill on the Net: Congress Enters the Information Age*, (Boston: AP Professional, 1996).

Committee on Information Technology Literacy, *Being Fluent with Information Technology*, (Washington: National Academy Press, 1999).

Richard Davis, *The Web of Politics: The Internet's Impact on the American Political System*, (New York: Oxford University Press, 1999).

Kenneth L. Hacker, *Digital Democracy: Issues of Theory and Practice*, (New York: Sage Publications, 2001).

Barry N. Hague and Brian Loader (eds.), *Digital Democracy: Discourse and Decision Making in the Information Age*, (New York: Routledge, 1999).

Kevin A. Hill and John E. Hughes, *Cyberpolitics: Citizen Activism in the Age of the Internet*, (New York: Rowman & Littlefield Publishing, 1998).

Elaine Ciulla Kamarck and Joseph S. Nye (eds.), *Democracy.Com: Governance in a Networked World*, (Hollis Publishing Company, 1999).

Lawrence K. Grossman, *The Electronic Republic: Reshaping Democracy in the Information Age*, (New York: Viking, 1995).

Anthony G. Wilhelm, *Democracy in the Digital Age: Challenges to Political Life in Cyberspace*, (New York: Routledge, 2000).