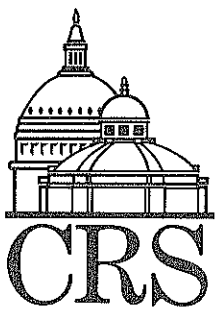
Order Code RL30745

CRS Report for Congress

Electronic Government: A Conceptual Overview

November 27, 2000

Harold C. Relyea
Specialist in American National Government
Government and Finance Division



Congressional Research Service • The Library of Congress

The Congressional Research Service works exclusively for the Congress, conducting research, analyzing legislation, and providing information at the request of committees, Members, and their staffs.

The Service makes such research available, without partisan bias, in many forms including studies, reports, compilations, digests, and background briefings. Upon request, CRS assists committees in analyzing legislative proposals and issues, and in assessing the possible effects of these proposals and their alternatives. The Service's senior specialists and subject analysts are also available for personal consultations in their respective fields of expertise.

Electronic Government: A Conceptual Overview

Summary

During the final decade of the 20th century, a new concept began to emerge in American political and governmental parlance—*electronic government*. Initially, the term was little more than a general recognition of a confluence of information technology developments and the application and use of these technologies by government entities. Subsequently, it has oftentimes been used as a symbol, an ambiguous reference to both current applications of information technology to government operations and a goal of realizing more efficient and economical performance of government functions. It is a dynamic concept of varying meaning and significance.

This report reviews the emerging concept of electronic government, or e-government; describes the policy environment defining and shaping it; and discusses some of the components of e-government implementation. A reading list of related CRS products is included. The report is exploratory, and will be updated as events recommend.

Contents

Background 1
Demand 3
Methodology 3
Findings 3
Conclusions 4
Policy Environment 5
Privacy Act 5
Paperwork Reduction Act 5
Computer Security Act 7
Computer Matching and Privacy Protection Act 7
Electronic Freedom of Information Amendments 8
Clinger-Cohen Act 9
E.O. 13011: Federal Information Technology Management 11
PDD 63: Critical Infrastructures Protection 14
Rehabilitation Act Amendments 16
Government Paperwork Elimination Act 17
Children's Online Privacy Protection Act 18
OMB Memoranda: Federal Web Site Privacy 19
Electronic Commerce 20
Implementation Components 23
Communication 23
Information Access 23
Service Delivery 24
Procurement 26
Security 26
Privacy 29
Management 30
Maintenance 32
Digital Divide 34
Emergency Response 35
Oversight 36
Public Views 37

Glossary 39

For Further Reading 41
CRS Documents 41
Other Documents 42

Electronic Government: A Conceptual Overview

During the final decade of the 20th century, a new concept began to emerge in American political and governmental parlance—*electronic government.* A joint report of the National Performance Review and the Government Information Technology Services Board, *Access America: Reengineering Through Information Technology*, issued February 3, 1997, introduced the new term.[1] Almost three years later, in a December 17, 1999, memorandum to the heads of executive departments and agencies, the President directed these officials to take certain actions in furtherance of "electronic government."[2] On May 18, 2000, Senators Fred D. Thompson (R-TN) and Joseph I. Lieberman (D-CT), the chair and ranking minority member, respectively, of the Senate Committee on Governmental Affairs, unveiled a Web site on electronic government, or e-government, to collect ideas from citizens on how the government might offer more services and better information online.[3] During June 2000, the concept became part of the campaign offerings of the two major party candidates for the presidency.[4]

As initially used in American public discourse, the e-government term was little more than a general recognition of a confluence of information technology (IT) developments and the application and use of these technologies by government entities. Subsequently, it has oftentimes been used as a symbol, an ambiguous reference to both current applications of IT to government operations and a goal of realizing more efficient and economical performance of government functions. It is a dynamic concept of varying meaning and significance.

Background

The conditions contributing to the e-government phenomenon were recognized at least three decades ago. Observations offered by the authors of a report of the

---

[1] Office of the Vice President, *Access America: Reengineering Through Information Technology; Report of the National Performance Review and the Government Information Technology Services Board* (Washington: GPO, 1997).

[2] The White House, Memorandum for the Heads of Executive Departments and Agencies, *Electronic Government* (Washington: Dec. 17, 1999).

[3] See Ben White, "Senators Go Looking for E-ideas," *Washington Post*, May 19, 2000, p. A29; the Web site may be accessed directly at [http://cct.georgetown.edu/development/eGov/] or through the committee Web site at [http://gov_affs.senate.gov]. Also see Shruti Date, "Senators' E-gov Site Comes to Fruition," *Government Computer News*, vol. 19, July 24, 2000, p. 62.

[4] See, for example, Christopher J. Dorobek, "Gore and Bush Make E-gov a Campaign Issue," *Government Computer News*, vol. 19, June 19, 2000, p. 6.

Commission on the Year 2000 of the American Academy of Arts and Sciences are informative in this regard. Concerning the executive branch, the report proffered:

> By the year 2000, despite the growth in the size and complexity of federal programs, the technological improvement of the computer, closed-circuit TV, facsimile transmission, and so on, will make it possible for the federal bureaucracy to carry out its functions much more efficiently and effectively than it can today, with no increase in total manpower.[5]

The use of information technologies was also seen as having critical importance for the legislative branch, constituting nothing less than "another aspect of congressional reform." Should "Congress continue to deny itself the tools of modern information technology and permit the Executive virtually to monopolize them," said the report, "Congress will ultimately destroy its power both to create policy and to oversee the Executive." Moreover, it was observed, the "technology revolution ... promises greater accessibility of senators and congressmen to their constituents, individually and collectively, and vice versa." Regarding this latter consideration, a warning was offered.

> Communications may become too close and constant, and act as a constricting force. For instance, by 2000 it will be easy to have virtually up-to-the-minute polls of the electorate on any given issue. But where does this instant-opinion development leave the senator and congressman?[6]

Such observations, however, should not obscure recognition that new information technologies have affected government operations in the past, as the following comment, penned in 1910, attests.

> Public officials, even in the United States, have been slow to change from the old-fashioned and more dignified use of written documents and uniformed messengers; but in the last ten years there has been a sweeping revolution in this respect. Government by telephone! This is a new idea that has already arrived in the more efficient departments of the Federal service. And as for the present Congress, that body has gone so far as to plan for a special system of its own, in both Houses, so that all official announcements may be heard by wire.[7]

The author, a respected Canadian editor and writer, also presciently noted that, "[n]ext to public officials, bankers were perhaps the last to accept the facilities of the telephone," because "[t]hey were slow to abandon the fallacy that no business can be

---

[5] William M. Capron, "The Executive Branch in the Year 2000," in Harvey S. Perloff, ed., *The Future of the U.S. Government: Toward the Year 2000* (New York: George Braziller, 1971), p. 307.

[6] John Brademus, "Congress in the Year 2000," in Harvey S. Perloff, ed., *The Future of the U.S. Government: Toward the Year 2000*, pp. 319-321.

[7] Herbert N. Casson, *The History of the Telephone* (Chicago: A. C. McClurg, 1910), pp. 201-202.

done without a written record."[8] Subscription to such a "fallacy" constitutes a basis for the concerns of some regarding the paperless transactions of e-government.

Demand

E-government is operational in the United States today at the local, state, and national government levels. What has been the public reaction thus far? An answer to this question may be found in a survey commissioned by NIC, a commercial provider of Internet services and solutions for more than 100 American and global government partners, including 12 federal agencies.[9] Survey results were released at a July 26, 2000, news conference at the National Press Club in Washington, D.C.

Methodology. For purposes of the survey, which was conducted by the Momentum Research Group of Cunningham Communication located in Austin, Texas, e-government was defined as "online government services, that is, any interaction one might have with any government body or agency, using the Internet or World Wide Web." The survey methodology included 406 interviews, of which three quarters fell into the citizen sector and one quarter fell into the business sector.[10]

Findings. The following summary of findings was provided by the survey report.

- Almost two out of three online adults (65 percent) have conducted an eGovernment transaction *at least* once.
- Almost one of five adults (20 percent) who use the Internet have conducted an eGovernment transaction in the *last thirty days*.
- Almost half of the citizen users (47 percent) reported they would like to use the Internet to renew their driver's license, vote in major elections (38 percent), and access one-stop shopping for all government services regardless of jurisdiction (36 percent).
- Almost half of the business users (43 percent) reported they would like to use the Internet to obtain or renew their professional license and access one-stop shopping to apply for all new business licenses and permits (39 percent).
- When given a choice, almost 3 out of 4 citizens (71 percent) and 3 out of 5 businesses (61 percent) prefer to pay convenience fees for services over taxpayer-funded eGovernment initiatives.

---

[8] Ibid., p. 203.

[9] NIC, *Benchmarking the eGovernment Revolution: Year 2000 Report on Citizen and Business Demand*, by the Momentum Research Group of Cunningham Communication (Reston, VA: NIC, 2000).

[10] Ibid., p. 34.

- Business users express a strong preference for a single Federal eGovernment portal, while citizens prefer to access information and services through their local eGovernment portal.[11]

- When asked whether governments and private companies should partner more on technology issues to provide eGovernment services, more than 2 out of 3 businesses (69 percent) and nearly half (49 percent) of citizens favor public-private partnerships.

- Only 1 in 3 (35 percent) eCommerce users and only 1 in 5 (20 percent) non-eCommerce users trust that the government will keep their records confidential.[12]

Conclusions. Based upon survey results, the report, generally finding that "eGovernment is widely accepted and seen as a growing trend and value to citizens and businesses nationwide," offered the following conclusions.

- Citizens and businesses are more satisfied with their eGovernment experience than with traditional government service delivery.

- Citizens and businesses understand and expect certain eGovernment benefits, such as efficiency, time savings and cost-effectiveness.

- The growth of eGovernment depends on education and awareness.[13]

- Citizens favor eGovernment initiatives that are closer to home at the state or local level.

- The services offered online are appropriate to the needs of citizens and business users and are offered at a price that they are willing to pay.

- Trust is the most critical issue facing the adoption of eGovernment. Government must successfully address issues of public trust for eGovernment to be successful in the long term.

- Citizens and businesses who have conducted eCommerce transactions are much more confident that privacy and trust are maintained in the electronic environment. As users begin to interact

---

[11] President Clinton announced plans for the creation of a single federal portal on June 24, 2000, during his first Internet Webcast; called FirstGov, the portal became operative on Sept. 22, and may be accessed at [http://www.firstgov.gov].

[12] NIC, *Benchmarking the eGovernment Revolution: Year 2000 Report on Citizen and Business Demand*, p. 3 (emphasis in original).

[13] For example, a $10,000 kiosk, recently installed in a District of Columbia supermarket and offering a wide variety of federal, state, and local government information and services, was almost totally ignored by passing shoppers, who were largely unaware of its purpose. See Manny Fernandez, "E-Government Not on Shopping List," *Washington Post*, Aug. 4, 2000, p. B4; Jennifer Surface, "Few Notice $10,000 Kiosk Set Up to Make Government Accessible," *Washington Times*, July 31, 2000, p. C2.

> with government online and experience the increased benefits, a greater degree of trust will be created.[14]

Policy Environment

A variety of policy instruments support and shape the e-government concept. In brief, they seek to promote the use of new information technology by government entities with a view to improving the efficiency and economy of government operations. In addition, they seek to ensure the proper management of these technologies and the systems they serve, their protection from physical harm, and the security and privacy of their information. Major policy developments in these regards are chronologically identified and summarized below.

Privacy Act. With the Privacy Act of 1974, Congress addressed several aspects of personal privacy protection.[15] First, it sustained some traditional major privacy principles. For example, an agency shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."[16]

Second, the statute provides an individual who is a citizen of the United States, or an alien lawfully admitted for permanent residence, with access and emendation arrangements for records maintained on him or her by most, but not all, federal agencies. General exemptions in this regard are provided for systems of records maintained by the Central Intelligence Agency and federal criminal law enforcement agencies.

Third, the statute embodies a number of principles of fair information practice. For example, it sets certain conditions concerning the disclosure of personally identifiable information; prescribes requirements for the accounting of certain disclosures of such information; requires agencies to "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs"; requires agencies to specify their authority and purposes for collecting personally identifiable information from an individual; requires agencies to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination"; and provides civil and criminal enforcement arrangements.

Paperwork Reduction Act. Replacing the ineffective Federal Reports Act of 1942, the original Paperwork Reduction Act of 1980 (PRA) was enacted largely to relieve the public from the mounting information collection and reporting

---

[14] NIC, *Benchmarking the eGovernment Revolution: Year 2000 Report on Citizen and Business Demand*, p. 4.

[15] 88 Stat. 1896; 5 U.S.C. 552a.

[16] 5 U.S.C. 552a(e)(7).

requirements of the federal government.[17] It also promoted coordinated information management activities on a governmentwide basis by the director of the Office of Management and Budget (OMB), and prescribed information management responsibilities for the executive agencies as well. The management focus of the PRA was sharpened with the 1986 amendments, which refined the concept of "information resources management"(IRM), defined as "the planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by agencies, and includes the management of information and related resources such as automatic data processing equipment."[18] This key term and its subset concepts received further definition and explanation in the PRA of 1995,[19] making IRM a tool for managing the contribution of information activities to program performance, and for managing related resources, such as personnel, equipment, funds, and technology.[20]

The evolution of the PRA reflects the beginning of an effort to manage electronic information and supporting IT better. A recodification of the 1980 statute, as amended, the PRA of 1995 specifies a full range of responsibilities for the director of OMB for all government information, regardless of form or format, throughout its entire life cycle. Regarding IT, the director, among other duties, is tasked with (1) developing and overseeing the implementation of policies, principles, standards, and guidelines for federal IT functions and activities, including periodic evaluations of major information systems; (2) overseeing the development and implementation of certain statutorily specified technology standards; (3) monitoring the effectiveness of, and compliance with, certain statutorily authorized technology directives; (4) coordinating the development and review by the OMB Office of Information and Regulatory Affairs (OIRA) of policy associated with federal procurement and acquisition of IT with the OMB Office of Federal Procurement Policy; (5) ensuring, through the review of agency budget proposals, IRM plans, and other means, both (a) the integration of IRM plans with program plans and budgets for the acquisition and use of IT by each agency, and (b) the efficiency and effectiveness of inter-agency IT initiatives to improve agency performance and the accomplishment of agency missions; and (6) promoting agency use of IT to improve the productivity, efficiency, and effectiveness of federal programs, including through the dissemination of public information and the reduction of information collection burdens on the public.

Similar responsibilities are specified for the agencies regarding government information, regardless of form or format, throughout its life cycle. With respect to IT, the agencies are tasked with (1) implementing and enforcing applicable governmentwide and agency IT management policies, principles, standards, and guidelines; (2) assuming responsibility and accountability for IT investments; (3) promoting the use of IT by the agency to improve the productivity, efficiency, and

---

[17] 94 Stat. 2812; 44 U.S.C. 3501 et seq.

[18] 100 Stat. 3341-336.

[19] 109 Stat. 165-166.

[20] See David Plocher, "The Paperwork Reduction Act of 1995: A Second Chance for Information Resources Management," *Government Information Quarterly*, vol. 13, no. 1, 1996, pp. 35-50.

effectiveness of agency programs, including the reduction of information collection burdens on the public and improved dissemination of public information; (4) proposing changes in legislation, regulations, and agency procedures to improve IT practices, including changes that improve the ability of the agency to use technology to reduce burden; and (5) assuming responsibility for maximizing the value and assessing and managing the risks of major information systems initiatives through a process that is both (a) integrated with budget, financial, and program management decisions, and (b) used to select, control, and evaluate the results of major information systems initiatives.

OMB governmentwide guidance on the implementation of the PRA and related policies is provided in Circular A-130, updated and reproduced in its entirety on February 8, 1996.[21] Appendices address federal agency responsibilities for maintaining records about individuals; cost accounting, cost recovery, and interagency sharing of information technology facilities; the security of federal automated information resources; and important key sections of the circular.

Computer Security Act. Recognizing the increasing use of computers by federal agencies and the vulnerability of computer-stored information, including personal information, to unauthorized access, Congress enacted the Computer Security Act of 1987.[22] The statute requires each federal agency to develop security plans for its computer systems containing sensitive information. Such plans are subject to review by the National Institute of Standards and Technology (NIST) of the Department of Commerce, and a summary, together with overall budget plans for IT, is filed with OMB. NIST is authorized to set security standards for all federal computer systems except those containing intelligence, cryptologic, or certain military information, or information specifically authorized under criteria established by an executive order or statute to be kept secret in the interest of national defense or foreign policy. The statute also mandates a Computer Systems Security and Privacy Advisory Board within the Department of Commerce to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy, and advise NIST and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems, among other duties. Each federal agency is directed to provide all employees involved with the management, use, or operation of its computer systems with mandatory periodic training in computer security awareness and accepted computer security practice.

Computer Matching and Privacy Protection Act. Congress amended the Privacy Act in 1988 to regulate the use of computer matching—the computerized comparison of records for the purpose of establishing or verifying eligibility for a federal benefit program or for recouping payments or delinquent debts under such programs—conducted by federal agencies or making use of federal records subject to the statute. The amendments were denominated the Computer Matching and

---

[21] See *Federal Register*, vol. 61, Feb. 20, 1996, pp. 6428-6453; the circular is also available from the OMB Web site at [http://www.whitehouse.gov/OMB/inforeg/index.html] under the heading "Information Policy and Technology."

[22] 101 Stat. 1724.

Privacy Protection Act of 1988.[23] A controversial matter for more than 10 years, computer matching had begun in 1977 at the Department of Health and Human Services. The effort, dubbed Project Match, compared welfare rolls in selected jurisdictions with federal payroll records in the same areas. The controversy surrounding this and similar computerized matches pitted privacy protection advocates, who alleged that personally identifiable data were being used for purposes other than those prompting their collection, against those using the technique to ferret out fraud, abuse, and the overpayment of federal benefits. As the practice subsequently became more widespread, controversy over its use grew.

The amendments regulate the use of computer matching by federal agencies involving personally identifiable records maintained in a system of records subject to the Privacy Act. Matches performed for statistical, research, law enforcement, tax, and certain other purposes are not subject to such regulation. In order for matches to occur, a written matching agreement, effectively creating a matching program, must be prepared specifying such details, explicitly required by the amendments, as the purpose and legal authority for the program; the justification for the program and the anticipated results, including a specific estimate of any savings; a description of the records being matched; procedures for providing individualized notice, at the time of application, to applicants for, and recipients of, financial assistance or payments under federal benefits programs and to applicants for and holders of positions as federal personnel that any information they provide may be subject to verification through the matching program; procedures for verifying information produced in the matching program; and procedures for the retention, security, and timely destruction of the records matched and for the security of the results of the matching program. Copies of such matching agreements are transmitted to congressional oversight committees and are available to the public upon request. Executive oversight of, and guidance for, matching programs is vested in the director of OMB. Notice of the establishment or revision of a matching program must be published in the *Federal Register* 30 days in advance of implementation.

The amendments also require every agency conducting or participating in a matching program to establish a Data Integrity Board, composed of senior agency officials, to oversee and coordinate program operations, including the execution of certain specified review, approval, and reporting responsibilities.

Agencies are prohibited from reducing, suspending, or terminating financial assistance to an individual without first verifying the accuracy of computerized data used in the matching program and without first giving the individual 30 days to contest the action.

Electronic Freedom of Information Amendments. In 1966, Congress enacted the Freedom of Information Act[24] (FOIA) to replace the public information section of the Administrative Procedure Act (APA), which was found to be ineffective in providing the public with a means of access to unpublished executive agency

---

[23] 102 Stat. 2507.

[24] 80 Stat. 250; 5 U.S.C. 552.

records.[25] Subsection (a) of the FOIA reiterates the requirements of the APA public information section that certain operational information—e.g., organization descriptions, delegations of final authority, and substantive rules of general policy—be published in the *Federal Register*.

Subsection (b) statutorily establishes a presumptive right of access by any person—individual or corporate, regardless of nationality—to identifiable, existing, unpublished records of federal agencies without having to demonstrate a need or even a reason for such a request. Subsection (b)(1)-(9) lists nine categories of information that may be exempted from the rule of disclosure. The burden of proof for withholding material sought by the public is placed upon the government. Denials of requests may be appealed to the head of the agency holding the sought records, and ultimately pursued in federal court.

The FOIA was subsequently amended in 1974, 1976, 1986, and 1996, the last modifications being the Electronic Freedom of Information Amendments (E-FOIA), which, among other changes, confirm the statute's applicability to records in electronic forms or formats, require that responsive materials be provided in the form or format sought by the requester, and mandate so-called electronic reading rooms which the public may access online to examine important and high visibility agency records.[26]

Clinger-Cohen Act. The PRA of 1995 was modified the following year by the 104th Congress with the adoption of new procurement reform and IT management legislation. A House bill (H.R. 1670) was introduced by Representative William F. Clinger, Jr. (R-PA), the chairman of the Committee on Government Reform and Oversight, on May 18, 1995. The measure was part of a procurement modernization effort that he had undertaken in furtherance of the reforms realized with the enactment of the Federal Acquisition Streamlining Act of 1994.[27] Referred to the Clinger committee, the bill was subsequently marked up and reported by the panel in July.[28] It came before the House on September 13 and, the following day, was passed, as amended, on a 423-0 recorded vote.[29]

A Senate procurement and IT management reform bill (S. 946) was introduced by Senator William S. Cohen (R-ME) on June 20, 1995. His bill grew out of a staff study he had directed during the previous Congress as the ranking minority member of the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs.[30] The bill was referred to the Committee on Governmental

---

[25] 60 Stat. 237.

[26] 110 Stat. 3048; 5 U.S.C. 552.

[27] 108 Stat. 3243.

[28] U.S. Congress, House Committee on Government Reform and Oversight, *Federal Acquisition Reform Act of 1995*, report to accompany H.R. 1670, 104th Cong., 1st sess., H.Rept. 104-222, Part 1 (Washington: GPO, 1995).

[29] *Congressional Record*, vol. 141, Sept. 14, 1995, p. 25027.

[30] See William S. Cohen, *Computer Chaos: Billions Wasted Buying Federal Computer*

(continued...)

Affairs. On August 4, during Senate consideration of the Department of Defense (DOD) authorization bill for FY1996 (S. 1026), Cohen offered an amendment, based on his procurement reform bill, that was accepted on a voice vote.[31] The Cohen amendment remained in the DOD authorization bill (H.R. 1530 amended with the language of S.1026) adopted by the Senate on September 6. The September 28 conference committee meeting on the legislation, with both Cohen and Clinger participating, provided an opportunity for reconciling their reform proposals into a mutually agreed upon package. The conferees' report, filed in the House on December 13, was approved in the House on December 15 on a 267-149 yea-nay vote, with the Senate agreeing four days later on a 51-43 yea-nay vote.

Although the Clinger-Cohen reforms drew no opposition from the White House, the President vetoed the DOD authorization bill for other reasons on December 28. An override attempt in the House, on January 3, 1996, failed on a 240-156 yea-nay vote. On January 5, managers of the DOD authorization legislation turned to one of three reserved legislative vehicles (S. 1124) created in September when the Senate completed action on the DOD authorization bill (H.R. 1530 amended with the language of S. 1026).[32] That day, the House passed the reserved bill (S. 1124) on a voice vote, then notified the Senate of its action and requested a conference, to which the Senate agreed. The conferees met on January 18; their report was filed in the House four days later.[33] The House agreed to the conference report on January 24 on a 287-129 yea-nay vote, the Senate giving its approval two days later on a 56-34 yea-nay vote. President Clinton signed the legislation on February 10.

Division D of the statute, concerning "Federal Acquisition Reform," was denominated the Federal Acquisition Reform Act of 1996.[34] Division E, concerning "Information Technology Management Reform," was known as the Information Technology Management Reform Act of 1996.[35] The two divisions were subsequently denominated the Clinger-Cohen Act.[36]

Repealing a section of the Automatic Data Processing Act,[37] the Clinger-Cohen Act makes each agency responsible for its own IT acquisition, and requires the

---

[30] (...continued)
Systems, Investigative Report (Washington: Oct. 12, 1994).

[31] *Congressional Record*, vol. 141, Aug. 4, 1995, pp. 22154-22158.

[32] See Ibid., Sept. 6, 1995, p. 23629.

[33] U.S. Congress, Conference Committees, 1996, *National Defense Authorization Act for Fiscal Year 1996*, conference report to accompany S. 1124, 104th Cong., 2nd sess., H.Rept. 104-450 (Washington: GPO, 1996).

[34] 110 Stat. 642.

[35] 110 Stat. 679.

[36] 110 Stat. 3009-393.

[37] 79 Stat. 1127.

purchase of the best and most cost effective technology available.[38] It also contains several provisions which either amend or gloss provisions of the PRA of 1995 as set out in chapter 35 of Title 44 of the U.S. Code.[39] Among the amendments is one establishing a chief information officer (CIO) in each agency, replacing the designated senior official mandated by the PRA at 44 U.S.C. 3506. Additional duties and qualifications of the CIO are prescribed in the Clinger-Cohen Act.

Other Clinger-Cohen Act provisions gloss the responsibilities prescribed in the PRA. The capital planning and investment control duties assigned to the OMB director by the Clinger-Cohen Act are to be performed, according to that statute, in fulfilling the director's IT responsibilities under 44 U.S.C. 3504(h) of the PRA. Similarly, the director is to "encourage the use of performance-based and results-based management" in fulfilling these same responsibilities. The Clinger-Cohen Act requires agency heads, in fulfilling their counterpart IT responsibilities assigned under 44 U.S.C. 3506(h) of the PRA, to "design and implement ... a process for maximizing the value and assessing and managing the risks of the information technology acquisitions of the ... agency" and to perform certain prescribed duties. Also, agency heads are to "identify in the strategic information resources management plan required under [44 U.S.C. 3506(b)(2)] any major information technology acquisition program, or any phase or increment of such a program, that has significantly deviated from the cost, performance, or schedule goals established for the program."

E.O. 13011: Federal Information Technology Management. Following the enactment of the PRA of 1995 and the Clinger-Cohen Act, President Clinton issued E.O. 13011 of July 16, 1996, to improve federal IT management and promote a coordinated approach to its application and use across the executive branch.[40] The directive prescribes, as a matter of policy, that executive agencies significantly improve the management of their information systems, including the acquisition of IT, by implementing the relevant provisions of the PRA and the Clinger-Cohen Act; refocus IT management to support directly their strategic missions, implement an investment review process that drives budget information and execution for information systems, and rethink and restructure the way they perform their functions before investing in IT to support that work; establish clear accountability for IRM activities by creating agency CIOs with the visibility and management responsibilities necessary to advise agency heads on the design, development, and implementation of those information systems; and cooperate in the use of IT to improve the productivity of federal programs and to provide a coordinated, interoperable, secure, and shared governmentwide infrastructure that is provided and supported by a diversity of private sector suppliers and a well-trained corps of IT professionals. Agencies are also directed to establish an interagency support structure that builds on existing successful

---

[38] 110 Stat. 186.

[39] The Clinger-Cohen Act provision (110 Stat. 680) repealed a section (40 U.S.C. 759) that had been appended to the Federal Property and Administrative Services Act by the Automatic Data Processing Act, which is popularly known as the Brooks Act; the repealed provision authorized the Administrator of General Services to coordinate and provide for the procurement, maintenance, and utilization of federal automatic data processing equipment.

[40] 3 C.F.R., 1996 Comp., pp. 202-209.

interagency efforts and provides expertise and advice to agencies; expand the skill and career development opportunities of IT professionals; improve the management and use of IT within and among agencies by developing IT procedures and standards and by identifying and sharing experiences, ideas, and promising practices; and provide innovative, multidisciplinary, project-specific support to agencies to enhance interoperability, minimize unnecessary duplication of effort, and capitalize on agency successes.

The directive details new responsibilities for agency heads, including effectively using IT to improve mission performance and service to the public. Strengthening the quality of decisions about the employment of information resources to meet mission needs through integrated analysis, planning, budgeting, and evaluation processes is another duty, including (1) determining, before making investments in new information systems, whether the government should be performing the function, if the private sector or another agency should support the function, and if the function needs to be or has been appropriately redesigned to improve its efficiency; (2) establishing mission-based performance measures for information systems investments, aligned with agency performance plans prepared pursuant to the Government Performance and Results Act;[41] (3) establishing agency-wide and project-level management structures and processes responsible and accountable for managing, selecting, controlling, and evaluating investments in information systems, with authority for terminating information systems when appropriate; (4) supporting appropriate training of personnel; and (5) seeking the advice of, participating in, and supporting the interagency support structure established elsewhere in the order.

Additional responsibilities include selecting CIOs with the experience and skills necessary to accomplish the duties prescribed in existing law and policy, and involving these officials in appropriate processes and decisions at the highest level of the agency; ensuring that the information security policies, procedures, and practices of the agency are adequate; structuring, where appropriate and in accordance with the Federal Acquisition Regulation and OMB guidance, major information systems investments into manageable projects as narrow in scope and brief in duration as practicable, consistent with the Clinger-Cohen Act; and, to the extent permitted by law, entering into a contract that provides for multiagency acquisitions of IT as an executive agent for the government in accordance with OMB direction.

The interagency support structure created by the directive includes the establishment of a Chief Information Officers Council to serve as the principal interagency forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources. The council is tasked with developing recommendations for overall federal IT management policy, procedures, and standards; sharing experiences, ideas, and promising practices, including work process redesign and the development of performance measures, to improve the management of information resources; identifying opportunities and making recommendations for, and sponsoring cooperation in, using information resources; assessing and addressing the hiring, training, classification, and professional development needs of the government with respect to IRM; making recommendations

---

[41] 107 Stat. 285; 31 U.S.C. 115 note.

and providing advice to appropriate executive agencies and organizations, including OMB, regarding the governmentwide strategic plan required by the PRA of 1995; and seeking the views of the Chief Financial Officers Council, the Government Information Technology Services Board, the Information Technology Resources Board, the Federal Procurement Council, industry, academia, and state and local governments, as appropriate, on matters of concern to the CIO Council. The membership of the council consists of the CIOs and deputy CIOs of 28 specified entities, two representatives from other agencies, and six other designated officials. It is chaired by the OMB deputy director for management.[42]

The order also mandated the Government Information Technology Services Board to ensure the continued implementation of the IT recommendations of the National Performance Review and to identify and promote the development of innovative technologies, standards, and practices among the agencies, state and local governments, and the private sector. Composed of executive agency personnel having proven expertise or accomplishments in the board's areas of responsibility, the panel was tasked with making recommendations to the CIO Council, OMB, and others, as appropriate, and otherwise help to create opportunities for cross-agency cooperation and intergovernmental approaches in using information resources to support common operational areas, developing and providing shared governmentwide infrastructure services, and developing standards and guidelines pertaining to federal information systems, consistent with the Computer Security Act, as amended. In April 2000, the board was absorbed by the new Electronic Government Committee of the CIO Council.[43]

In addition, the order establishes the Information Technology Resources Board to provide independent assessments to assist in the development, acquisition, and management of selected major information systems and to provide recommendations to agency heads and OMB as appropriate. The board is tasked with reviewing, at the request of an agency and OMB, specific information systems proposed or under development and making recommendations regarding the status of such systems or next steps; publicizing lessons learned and promising practices based on information systems reviewed by the board; and seeking, as appropriate, the views of experts from industry, academia, and state and local governments on matters of concern to the board. The panel's membership is composed of agency personnel, based upon their knowledge of IT, programs, or acquisition management within executive agencies.

Finally, the order sets out certain responsibilities for selected executive branch officials. The OMB director is tasked with evaluating agency IRM practices and, as part of the budget process, analyzing, tracking, and evaluating the risks and results of all major capital investments for information systems; notifying an agency if he or she believes that a major information system requires outside assistance; providing guidance on the implementation of the order and on the management of information resources to the agencies and to the boards established by the directive; and evaluating

---

[42] The CIO Council Web site may be found at [http://www.cio.gov].

[43] Christopher J. Dorobek, "CIO Council's New Committee Absorbs GITS Board," *Government Computer News*, vol. 19, Apr. 17, 2000, p. 16.

the effectiveness of the management structure prescribed in the order after three years and making recommendations for appropriate changes.

Under the direction of OMB, the Administrator of General Services, among other duties, develops, maintains, and disseminates for agency use, as requested by OMB or the agencies, recommended methods and strategies for the development and acquisition of IT; conducts and manages outreach programs in cooperation with agency managers; serves as a focal point for liaison on IRM with state and local governments and nongovernmental international organizations; supports the Secretary of State in liaison, consultation, and negotiation activities with intergovernmental organizations regarding IRM matters; assists OMB, as requested, in evaluating agencies' performance-based management tracking systems and their achievement of cost, schedule, and performance goals; and provides support and assistance to the interagency groups established by the order.

The Secretary of Commerce is responsible for carrying out the standards responsibilities assigned by the Computer Security Act, as amended by the Clinger-Cohen Act, taking into consideration the recommendations of the agencies, the CIO Council, and the Information Technology Resources Board. The Secretary of State, as noted above, has responsibility for liaison, consultation, and negotiation with foreign governments and intergovernmental organizations on all matters related to IRM; ensures, in consultation with the Secretary of Commerce, that the United States is represented in the development of international standards and recommendations affecting IT; and advises the OMB director on the development of United States positions and policies on international information policy and technology issues affecting federal government activities and the development of international IT standards.

PDD 63: Critical Infrastructures Protection. Concerned about the vulnerabilities of certain critical national infrastructures—including the telecommunications system—to physical and cyber attack, President Clinton, with E.O. 13010 of July 15, 1996, established the President's Commission on Critical Infrastructure Protection.[44] The temporary study panel was tasked with assessing the scope and nature of the vulnerabilities of, and threats to, critical infrastructures; determining what legal and policy issues are raised by efforts to protect critical infrastructures and assessing how these issues should be addressed; recommending a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation; and proposing any statutory or regulatory changes necessary to effect its recommendations. The commission produced 12 special topical reports and submitted its final report, offering many recommendations, on October 13, 1997.[45]

---

[44] 3 C.F.R., 1996 Comp., pp. 198-202; according to E.O. 13010, a "cyber" attack involves "electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures."

[45] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington: GPO, 1997); this report and other documents relevant to the commission's activities are available at

(continued...)

On May 22, 1998, the White House issued documents concerning Presidential Decision Directive 63 (PDD 63), a security classified policy instrument on critical infrastructure protection.[46] (The directive was recently declassified and made available for public examination.[47]) PDD 63 is the product of an interagency evaluation of the recommendations of the President's Commission on Critical Infrastructure Protection with a view to producing a workable and innovative framework for critical infrastructure protection. The directive sets a goal of a reliable, interconnected, and secure information system infrastructure by 2003, and significantly increased security for government systems by 2000. To assist with the realization of this goal, PDD 63 establishes four new entities:

- a National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, whose responsibilities include not only critical infrastructure protection, but also safeguarding against foreign terrorism and threats of domestic mass destruction, including biological weapons;

- a National Infrastructure Protection Center at the Federal Bureau of Investigation, which involves representatives from the bureau, the Department of Defense, the United States Secret Service, the Department of Energy, the Department of Transportation, the intelligence community, and the private sector in an information sharing and collaboration effort, and which also provides the principal means of facilitating and coordinating the federal response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts;

- a National Infrastructure Assurance Council, composed of private sector experts and state and local government officials, to provide guidance for a national plan for critical infrastructure protection;[48] and

- a Critical Infrastructure Assurance Office to provide support for the National Coordinator's work with government agencies and the private sector in developing a national plan for critical infrastructure protection, and to help coordinate a national education and awareness program, and legislative and public affairs activities.

---

[45] (...continued)
[http://www.ciao.gov/PCCIP/pccip_documents.htm].

[46] A fact sheet, a white paper, and a press briefing transcript on PDD 63 are available from the White House Web site at [http://www.whitehouse.gov/library/index.html] through a search of the "Archive of All White House Documents"; part of a series of national security policy instruments, PDDs and their predecessors are discussed in U.S. Library of Congress, Congressional Research Service, *Presidential Directives: Background and Overview*, by Harold C. Relyea, CRS Report 98-611 (Washington: July 16, 1998), pp. 8-11.

[47] The full text of PDD 63 is available at [http://www.fas.org/irp/offdocs/pdd/pdd-63.htm].

[48] Formally chartered by E.O. 13130 of July 14, 1999, 3 C.F.R., 1999 Comp., pp. 203-204.

The directive also encourages the creation of Information Sharing and Analysis Centers in partnership with the private sector and modeled on the Centers for Disease Control and Prevention.

Among the immediate tasks set by PDD 63, to be completed within the first 180 days, were the development of a critical infrastructure protection plan by each federal department and agency for itself; initial vulnerability analyses of each sector of the economy and the government that might be a target of infrastructure attack intended to damage the United States significantly; an initial remedial plan, based upon the vulnerability analysis, for each sector; a system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage; and the development and implementation of a plan for enhancing intelligence collection and analysis of the foreign threat to the critical infrastructure of the United States.

The center piece of the efforts launched with PDD 63 is a national plan to serve as a blueprint for establishing a critical infrastructure protection capability. Version one, the National Plan for Information Systems Protection, was unveiled on January 7, 2000.[49] Subtitled "an invitation to a dialogue," version one of the plan has been offered for public comment.[50] As President Clinton explained in his introduction:

> The National Plan for Information Systems Protection is the first major element of a more comprehensive effort. The Plan for cyber defense will evolve and be updated as we deepen our knowledge of our vulnerabilities and the emerging threats. It presents a comprehensive vision creating the necessary safeguards to protect the critical sectors of our economy, national security, public health, and safety.[51]

Rehabilitation Act Amendments. Among the 1998 amendments to the Rehabilitation Act of 1973 adopted by Congress is a new subsection requiring federal agencies to procure, maintain, and use electronic and information technology that provides individuals with disabilities, including both federal employees and members of the public, with accessibility comparable to what is available to individuals without disabilities.[52] The Architectural and Transportation Barriers Compliance Board, known as the Access Board, was tasked with developing access standards to

---

[49] The full text and executive summary of the national plan are available from the Critical Infrastructure Assurance Office Web site at [http://www.ciao.gov] in the "CIAO Document Library."

[50] Comments are to be directed to the Critical Infrastructure Assurance Office, which reports on national plan activities through its Web site at [http://www.ciao.gov].

[51] The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue* (Washington: Jan. 7, 2000), p. iii.

[52] The Rehabilitation Act Amendments of 1998 constituted Title IV of the Workforce Investment Act of 1998, 112 Stat. 936; the electronic and information technology access requirement was appended to the Rehabilitation Act as section 508, 112 Stat 1203, at 29 U.S.C. 794(d); the Rehabilitation Act was originally enacted in 1973, 87 Stat. 355, at 29 U.S.C. 701 et seq.

implement the new requirement. The amendments anticipated that the board would issue final access standards in February 2000 and the electronic and information technology access requirement would become effective on August 7, 2000. However, the Access Board did not publish proposed standards for electronic and information technology for public comment until March 31, 2000.[53] Provision was subsequently made in the Military Construction Appropriations Act for Fiscal Year 2001 to delay the effective date of the electronic and information technology access requirement until six months after the date of the publication of the board's final standards.[54] While the access requirement is expected to become effective by mid-2001, federal agencies are actively preparing to ensure that not only their Web sites, but also their internal software programs are in compliance,[55] and free software for testing Web site accessibility recently became available to ease agency burden and cost.[56] In a related development, President Clinton issued executive orders on July 26, 2000, setting a goal for federal agencies to hire 100,000 qualified individuals with disabilities over the next five years and requiring the agencies to accommodate federal employees with disabilities in the workplace better.[57]

Government Paperwork Elimination Act. Additional amendments to the PRA were enacted in 1998 as the Government Paperwork Elimination Act (GPEA). The legislation (S. 2107) was introduced by Senator Spencer Abraham (R-MI) in May and was referred to the Committee on Commerce, where it was redrafted. According to the committee report, which was filed on September 17, the revised bill "would require Federal agencies to make electronic versions of their forms available online and would allow individuals and businesses to use electronic signatures to file these forms electronically." Continuing, the report indicated that the intent of the legislation "is to provide a framework for reliable and secure electronic transactions with the Federal government while remaining 'technology neutral' and not inappropriately favoring one industry over another."[58] The Senate subsequently approved the bill on October 15.

By this time, however, the 105th Congress was moving toward final adjournment. Consequently, agreement was reached that the language of the noncontroversial Senate bill would be attached, as Title 17, to the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, which cleared both houses of Congress and

---

[53] *Federal Register*, vol. 65, Mar. 31, 2000, pp. 17346-17367; the proposed standards also are available from the Access Board Web site at [http://www.access-board.gov/sec508/508index.htm].

[54] 114 Stat. 555.

[55] Carrie Johnson, "Agencies Act to Ease Use of Internet by Disabled," *Washington Post*, Aug. 24, 2000, p. A23.

[56] Steve Graves, "Bobby Blows Whistle on Inaccessible Web Pages," *Government Computer News*, vol. 19, Sept. 4, 2000, pp. 1, 60-61.

[57] E.O. 13163 and E.O. 13164 in *Federal Register*, vol. 65, July 28, 2000, pp. 46563-46566.

[58] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Government Paperwork Elimination Act*, a report to accompany S. 2107, 105th Cong., 2nd sess., S.Rept. 105-335 (Washington: GPO, 1998), p. 1.

was signed into law by President Clinton on October 21, 1998.[59] As enacted, the GPEA makes the director of OMB responsible for providing governmentwide direction and oversight regarding "the acquisition and use of information technology, including alternative information technologies that provide for electronic submission, maintenance, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures."[60] In fulfilling this responsibility, the director, in consultation with the National Telecommunications and Information Administration (NTIA) of the Department of Commerce, is tasked with developing, in accordance with prescribed requirements, procedures for the use and acceptance of electronic signatures by the executive departments and agencies. A five-year deadline is prescribed for the agencies to implement these procedures.[61]

The director of OMB is also tasked by the GPEA to "develop procedures to permit private employers to store and file electronically with Executive agencies forms containing information pertaining to the employees of such employers."[62] In addition, the director, in cooperation with NTIA, is to conduct an ongoing study of the use of electronic signatures under the GPEA, with attention to paperwork reduction and electronic commerce, individual privacy, and the security and authenticity of transactions. The results of this study are to be reported periodically to Congress.

Finally, electronic records submitted or maintained in accordance with GPEA procedures, "or electronic signatures or other forms of electronic authentication used in accordance with such procedures, shall not be denied legal effect, validity, or enforceability because such records are in electronic form." The act further specifies: "Except as provided by law, information collected in the provision of electronic signature services for communications with an executive agency ... shall only be used or disclosed by persons who obtain, collect, or maintain such information as a business or government practice, for the purpose of facilitating such communications, or with the prior affirmative consent of the person about whom the information pertains."[63]

Children's Online Privacy Protection Act. Although the Clinton Administration and many Members of Congress preferred to rely upon industry self regulation for realizing Internet privacy protection, frustration with the industry's slow response regarding minors led to the enactment of the Children's Online Privacy Protection Act of 1998 (COPPA) as part of the Omnibus Consolidated and Emergency Supplemental

---

[59] See 112 Stat. 2681-749.

[60] 44 U.S.C. 3504(a)(1)(B)(vi), as amended.

[61] The final version of OMB procedures and guidance for implementing the GPEA was published in *Federal Register*, vol. 65, May 2, 2000, pp. 25508-25521, and a memorandum on the preparation and submission of agency plans to implement the statute was issued on July 25; both documents are available from the OMB Web site at [http://www.whitehouse.gov/OMB/inforeg/index.html] under the heading "Information Policy and Technology."

[62] 112 Stat. 2681-750.

[63] 112 Stat. 2681-751.

Appropriations Act, 1999.[64] The statute requires the operator of a commercial Web site or online service targeted at children under the age of 13 to provide clear notice of information collection and use practices; to obtain verifiable parental consent prior to collecting, using, and disseminating personal information about children under 13; and to provide parents access to their children's personal information and the option to prevent its further use. On October 20, 1999, the Federal Trade Commission issued a final rule to implement the COPPA, which went into effect on April 21, 2000.[65] The statute authorizes the commission to bring enforcement actions and impose civil penalties for violations of the rule in the same manner as for its other rules. A June 22, 2000, Web site privacy memorandum from the OMB director to the heads of executive departments and agencies, discussed below, prescribed, as a matter of policy, compliance with the standards set forth in the COPPA by federal agencies and contractors operating on behalf of agencies.

OMB Memoranda: Federal Web Site Privacy. A June 2, 1999, memorandum from the OMB director to the heads of executive departments and agencies directs the posting of clear privacy policies on federal Web sites and provides guidance for this action.[66] Such policies "must clearly and concisely inform visitors to the site what information the agency collects about individuals, why the agency collects it, and how the agency will use it." Also, they "must be clearly labeled and easily accessed when someone visits a web site," according to the memorandum. Agencies are reminded that, pursuant to the Privacy Act, they must protect an individual's right to privacy when they collect personal information.

A June 22, 2000, followup memorandum was issued by OMB after press disclosures that the National Drug Control Policy Office, an agency within the Executive Office of the President, was secretly tracking visitors to its Web site through the use of computer software known as "cookies."[67] Addressing this revelation, it said:

> Particular privacy concerns may be raised when uses of web technology can track the activities of users over time and across different web sites. These concerns are especially great where individuals who have come to government web sites do not have clear and conspicuous notice of any such tracking activities. "Cookies"—small bits of software that are placed on a web user's hard drive—are a principal example of current web technology that can be used in this way. The guidance issued on June 2, 1999, provided that agencies could only use "cookies" or other automatic means of collecting information if they gave clear notice of those activities.
>
> Because of the unique laws and traditions abut government access to citizens' personal information, the presumption should be that "cookies" will not be used at

---

[64] 112 Stat. 2681-728; 15 U.S.C. 6501-6506.

[65] *Federal Register*, vol. 64, Nov. 3, 1999, pp. 59888-59915.

[66] This memorandum is available from the OMB Web site at [http://www.whitehouse.gov/OMB/inforeg/index.html] under the heading "Information Policy and Technology."

[67] See John F. Harris and John Schwartz, "Anti-Drug Web Site Tracks Visitors," *Washington Post*, June 22, 2000, p. A23; Lance Gay, "White House Uses Drug-Message Site to Track Inquiries," *Washington Times*, June 21, 2000, p. A3.

technologies has not only revolutionized the storage, retrieval, and sharing of information, but also, in the considered view of many, produced an information economy resulting from commercial transactions on the Internet. The federal government is a participant in e-commerce, and statutes such as the GPEA, discussed above, reflect encouragement of this development.

Among the first Clinton Administration initiatives in furtherance of government participation in e-commerce was the June 15, 1995, unveiling of the U.S. Business Advisor, a new online computer service directly linking the federal government to American business.[69] The new service was announced by the President and Vice President during the White House Conference on Small Business being held at the Washington Hilton Hotel.[70] An upgraded and improved version of the U.S. Business Advisor, providing users with one-stop electronic access to more than 60 different federal organizations that assist or regulate businesses, was announced by Vice President Gore on February 13, 1996.

On July 1, 1997, President Clinton released a report, *A Framework for Global Electronic Commerce*, expressing five operating principles that the administration would follow in fostering e-commerce, and designating lead federal agencies in key policy areas.[71] These principles are as follow.

- The private sector should lead.

---

[68] This memorandum is available from the OMB Web site at [http://www.whitehouse.gov/OMB/inforeg/index.htm] under the heading "Information Policy and Technology"; for critique of the OMB memorandum, see Walter R. Houser, "OMB Cookie Memo Crumbles Under Its Own Weight," *Government Computer News*, vol. 19, July 24, 2000, p. 21, and "As It's Written, OMB Policy on Cookies is Half-baked," *Government Computer News*, vol. 19, Nov. 6, 2000, p. 27.

[69] U.S. Business Advisor may be found at [http://www.business.gov].

[70] Press releases on the Clinton Administration developments discussed here are available from the virtual library of the White House Web site at [http://www.whitehouse.gov/library/index.html].

[71] President's Information Infrastructure Task Force, *A Framework for Global Electronic Commerce* (Washington: July 1, 1997), available from the National Institute of Standards and Technology Web site at [http://www.iitf.nist.gov/eleccomm/ecomm.htm].

- Governments should avoid undue restrictions on electronic commerce.
- Where government involvement is needed, its aim should be to support and enforce a predictable minimalist, consistent and simple legal environment for commerce.
- Governments should recognize the unique qualities of the Internet.
- Electronic commerce on the Internet should be facilitated on a global basis.

In his remarks announcing the release of the report, the President indicated he was directing all federal department and agency heads to review the policies of their organization that affect global electronic commerce with a view to assuring that they are consistent with the five core principles of the report. Cabinet members were being directed to enter upon achieving some of the administration's key objectives within the next year, he said, and relevant agencies were being called upon to work with the Department of Commerce, industry, and law enforcement agencies to assure that Americans can conduct their business affairs in a secure environment. The assistance of the private sector was being sought to meet "one of the greatest challenges of electronic commerce: ensuring that we develop effective methods of protecting the privacy of every American, especially children who use the Internet." Specific assignments and taskings in these regards may be found in a July 1 presidential memorandum to the heads of executive departments and agencies on the subject of electronic commerce. A November 30, 1998, memorandum to the heads of executive departments and agencies assigned additional responsibilities to the Assistant to the President for Economic Policy, the Secretaries of Commerce and State, and the administrator of the Small Business Administration.

On January 24, 1999, the President and Vice President announced an Information Technology for the 21st Century (IT2) initiative for which $336 million was proposed to fund three kinds of activities.

- Long-term information technology research that will lead to fundamental advances in computing and communications, in the same way that government investment beginning in the 1960's led to today's Internet;
- Advanced computing for science, engineering and the Nation that will lead to breakthroughs such as reducing the time required to develop life-saving drugs; designing cleaner, more efficient engines; and more accurately predicting tornadoes; and
- Research on the economic and social implications of the Information Revolution, and efforts to help train additional IT workers at our universities.

The significance of IT2 was underscored in a February report of the President's Information Technology Advisory Committee, which, in relevant part, said:

> While the importance of information technology to the future of the economy and the government is clear, it may not be immediately obvious that government investment is needed to ensure continued progress.
>
> We cannot rely on industry to fund the needed research because they necessarily focus, in view of economic realities, on the short term. Industry cannot and will not invest in solving problems of importance to society as a whole unless such investments make sense from a business perspective.
>
> Information technology research is essential for the continued growth of the economy and for the solution of some of the most critical problems facing the Nation. Unless steps are taken now to reinvigorate Federal research in this critical area, we are very likely to see a significant reduction in the rate of progress over the coming decades. The cost to the Nation of such a reduction will be significantly greater than the investment needed to address the problem.[72]

In a November 29, 1999, memorandum to the heads of executive departments and agencies, President Clinton directed each federal agency, including independent regulatory agencies, to assist a working group on electronic commerce with identifying any provision of law administered by the agencies, and any regulation issued by them, that may impose a barrier to electronic transactions or otherwise impede the conduct of commerce online or by electronic means. They were also tasked with recommending how such laws or regulations might be revised to allow electronic commerce to proceed while maintaining protection of the public interest. A similar exercise was to be conducted with representatives of state and local government by the working group.

The heads of executive departments and agencies were informed of Clinton Administration efforts to address the so-called digital divide in a December 9, 1999, presidential memorandum. The digital divide is a reference to the perceived disparity that results from portions of the population not having the ability to use IT due to a lack of access and/or skill. Among the actions directed, the memorandum indicated, were the development of a national strategy for making computers and the Internet accessible to all Americans; expansion of the federal community technology centers network to provide low-income citizens with access to IT; encouragement of the development of IT applications that would help enable low-income citizens to start and manage their own small businesses; and use of training to upgrade the IT skills of the American workforce, particularly workers living in disadvantaged urban and rural communities.

A December 17, 1999, memorandum to the heads of executive departments and agencies directed them, among other actions, to make available online, by December 2000, to the maximum extent possible, the forms needed for the top 500 government services used by the public; to make transactions with the federal government performable online, with online processing, by October 2003; and to promote the use of electronic commerce, where appropriate, for faster, cheaper ordering on federal procurements.

---

[72] U.S. President's Information Technology Advisory Committee, *Report to the President: Information Technology Research: Investing in Our Future* (Washington: February 1999), pp. 6-7; the report is available at [http://www.ccic.gov/ac].

Implementation Components

In the paragraphs below, some of the principal components of the electronic government concept are identified and discussed.

Communication. Traditionally, communication between an agency and the public has occurred through written and verbal exchanges, the latter being either in person or by telephone. Electronic government introduces the prospect of such communication occurring via the Internet, through Web site visitation or electronic mail. An agency Web site may offer forms or applications which can be completed and filed online, prompting the agency to respond to the communique. Federal agencies generally have managed electronic mail, or e-mail, communication with the public in a manner analogous to telephone communication with the public. Call centers, which serve as an agency contact point for the public (viewed, in a market context, as "customers") via a toll-free telephone number, are often the agency receiving point for e-mail from the public. Indeed, there is growing recognition of the importance of such centers for realizing "customer" satisfaction.[73]

Just as federal agencies traditionally have been guarded about publicly disclosing the direct telephone numbers of senior agency officials, so too have they exhibited reluctance to reveal the e-mail addresses of such officials. However, this situation is changing, in both matters, as various commercially produced staff directories readily reveal.

Information Access. From 1789 through the first decade of the 20th century, the federal government seems to have largely satisfied the information needs of the American people through the publication of official documents. With the rise of the administrative state during the administration of President Woodrow Wilson, this situation began to change. Government began to become more complex, more intrusive, and more regulative of more aspects of social and economic intercourse. These conditions intensified during the New Deal and the prosecution of World War II. In response, a growing volume of public requests for unpublished information greeted an expanding bureaucracy, which too often appeared to be indifferent to, if not scornful of, such entreaties. In 1946, Congress sought to provide some relief with a section of the Administrative Procedure Act (APA) prescribing a general procedure for the request of public information from the executive departments and agencies.[74] Unfortunately, the section gave the agencies broad discretionary authority to withhold requested information and failed to provide an action-forcing mechanism to settle disputes outside of the refusing agency.

Congress returned to the information access issue in the latter half of the 1950s. After several years of investigating the problems and developing remedial legislation,

---

[73] Christopher J. Dorobek, "Call Centers, User Satisfaction Are Crucial to E-gov Success, Experts Say," *Government Computer News*, vol. 19, May 22, 2000, p. 12; also see U.S. General Accounting Office, *Customer Service: Human Capital Management at Selected Public and Private Call Centers*, GAO Report GAO/GGD-00-161 (Washington: August 2000),

[74] 60 Stat. 237.

it enacted the FOIA in 1966, discussed above, to replace the ineffective public information section of the APA.[75] Amendments to the act in 1996, among other modifications, confirm the statute's applicability to records in electronic forms or formats, require that responsive materials be provided in the form or format sought by the requester, and mandate so-called electronic reading rooms which the public may access online to examine important and high visibility agency records.[76]

Three years earlier, President Clinton, in an October 4, 1993, memorandum to the heads of executive departments and agencies asking them "to renew their commitment to the Freedom of Information Act, to its underlying principles of government openness, and to its sound administration," reminded them that "our commitment to openness requires more than merely responding to requests from the public. Each agency has a responsibility to distribute information on its own initiative, and to enhance public access through the use of electronic information systems."[77]

Information access, in the context of electronic government, rests upon these policies. Agencies have made a large amount of information accessible to the public through their Web sites, and will continue to do so. For example, the Federal Aviation Administration provides various kinds of information for air passengers, including weather related delays reported at major U.S. airports.[78] Another popular Web site is the *Healthfinder* page maintained by the Department of Health and Human Services and covering more than 1,000 health-related topics.[79] For those interested in exploring national park facilities by theme and location, the National Park Service has created *Visit Your Parks*.[80] However, at least two important matters remain to be addressed. One concerns the length of time documents or data are available on an agency Web site, and their subsequent retrieval from archival status through the Web site. The other concerns the ability to make online requests, pursuant to the FOIA, through the agency Web site, for records and information not otherwise made accessible through the Web site.

Service Delivery. A great many federal departments and agencies have been created to provide various services to the American people and businesses. One of the oldest and most visible of these is the United States Postal Service (USPS), which traces its origins to 1775. Ironically, as federal entities actively seek to provide their services through Internet transactions, the Postal Service appears to be among the first

---

[75] 80 Stat. 250, subsequently amended and codified at 5 U.S.C. 552.

[76] 110 Stat. 3048; 5 U.S.C. 552.

[77] U.S. National Archives and Records Administration, Office of the Federal Register, *Public Papers of the Presidents of the United States: William J. Clinton, 1993* (Washington: GPO, 1994), p. 1685.

[78] The Federal Aviation Administration's passenger information page may be found at [http://www.faa.gov/passinfo.htm].

[79] The Department of Health and Human Services' *Healthfinder* page may be found at [http://www.healthfinder.gov/].

[80] The National Park Service's *Visit Your Parks* page may be found at [http://www.nps.goc/parks/search.htm].

to be negatively impacted by this development. The mail carrier expects to lose about $180 million in revenue in 2000 as a consequence of half a billion federal checks being delivered electronically rather than by the USPS.[81] Examples of federal agencies using electronic service delivery to their advantage include the Department of Education, which provides a *Free Application for Federal Student Aid* Web site where students and parents can log on and apply for financial aid for college.[82] The Bureau of Public Debt, Department of the Treasury, maintains a Web site where visitors may purchase Treasury bills and bonds with a credit card or bank transfer, determine current redemption rates and interest earned on their investments, obtain nearly instant data on auction results and debt buyback programs, and get an exact, daily tally on the national debt.[83] At the Department of the Interior, the Bureau of Land Management maintains a Web site in furtherance of its wild horse adoption program. Potential adopters can log on to *Adopt-a-Horse Program*, view color photos of the potential adoptees, and electronically apply for permission to adopt.[84] The Department of Housing and Urban Development (HUD) has created an online realty store where interested individuals can shop for and bid on HUD-owned homes.[85] Applications for Social Security retirement benefits may now be filed electronically, but may still be made via a toll-free telephone number or in person.[86]

Of interest for reasons of both information access and service delivery is the launching of FirstGov, the single federal portal to all national government Web sites, on September 22, 2000.[87] President Clinton announced plans for the undertaking in June, and efforts at creating the portal began in August, the final objective being to perform high-speed searches of an estimated 100 million Web pages at 25,000 federal sites.[88] At launch, FirstGov connected users to 27 million Web pages and attracted an estimated 250,000 users during its first four days of operation. It will be administered by the nonprofit Federal Search Foundation, which created the huge FirstGov search engine, for two years, after which the government can operate it or outsource its

---

[81] William Matthews, "E-business Shortchanges USPS," *Federal Computer Week*, vol. 14, Sept. 25, 2000, p. 14.

[82] The Department of Education's *Free Application for Federal Student Aid* Web site may be found at [http://www.fafsa.ed.gov/].

[83] The Bureau of Public Debt Web site may be found at [http://www.publicdebt.treas.gov/].

[84] The Bureau of Land Management's *Adopt-a-Horse Program* Web site may be found at [http://www.adoptahorse.blm.gov/].

[85] The Department of Housing and Urban Development's homes for sale page may be found at [http://www.hud.gov/local/sams/ctznhome.html], and other information in this regard may be found on the department's home Web site at [http://www.hud.gov] by consulting "Own a Home" on the search/index page.

[86] Application for Social Security retirement benefits made be made at [http://www.ssa.gov/applytoretire] or by calling 1-800-772-1213.

[87] FirstGov may be found at [http://www.FirstGov.gov].

[88] "FirstGov Team Gets Under Way," *Government Computer News*, vol. 19, Aug. 21, 2000, p. 3.

management.[89] An initial congressional hearing on FirstGov, held by the House Subcommittee on Government Management, Information, and Technology on October 2, revealed GAO concern about the portal's vulnerability to hackers, cyberterrorists, and others with malicious intent; a public interest group's initial satisfaction with the innovation; industry perception of the portal as unwelcome competition; and general uneasiness about the future operation of FirstGov and ownership of its indexed database after the Federal Search Foundation ceases management.[90] Industry concerns were heard again a few days after this hearing when the Computer and Communications Industry Association, a trade group representing equipment manufacturers, software developers, and telecommunications and online service providers, among others, released a study it had funded which was critical of some federal online services that "encroach dangerously on businesses already served by private enterprise."[91]

Procurement. Apart from engaging in sales to the public, federal departments and agencies purchase goods and services from the private sector. Details regarding such procurement are offered on agency Web sites in various ways, including bid opportunities and placement arrangements, special contracts, and unsolicited proposals. Procurement opportunities for small businesses and for women- and minority-owned businesses are often identified, as are acquisitions of particular goods and services, such as information technology. Among the major federal procurement agencies maintaining Web sites for this function are the Defense Logistics Agency,[92] the General Services Administration,[93] and the National Aeronautics and Space Administration.[94]

Security. For electronic government, security has several dimensions. Continuing efforts are being made to protect Internet transactions among government entities and between those entities and the public against obstruction, diversion, interception, and falsification. The use of encryption and digital signature capabilities is being applied to assure better the integrity of such transactions. However, the Internet infrastructure must also be safeguarded; agency Web site offerings must be protected against "hacking"; and agency information technology systems, including Web sites and computers, must be regularly cleared of viruses, so-called "Trojan horses," and similar transgressing and destructive contaminants. Finally, agency storage of electronic data

---

[89] Tony Lee Orr, "FirstGov Connects Users to 27 Million Web Pages," *Government Computer News*, vol. 19, Oct. 2, 2000, p. 3.

[90] U.S. Congress, House Committee on Government Reform, Subcommittee on Government Management, Information, and Technology, *FirstGov.gov: Is It a Good Idea?*, hearing, 106th Cong., 2nd sess., Oct. 2, 2000 (Washington: transcript awaiting publication).

[91] See Joseph E. Stiglitz, Peter R. Orszag, and Jonathan M. Orszag, *The Role of Government in a Digital Age*, commissioned by the Computer and Communications Industry Association (Washington: October 2000), available at [http://www.ccianet.org/digitalgovstudy/main.html]; Curt Suplee, "Government E-Ventures Hit as Rivals to Business," *Washington Post*, Oct. 13, 2000, p. A37.

[92] See the Defense Logistics Agency's Web site at [http://dla.mil/].

[93] See the General Services Administration's Web site at [http://www.gsa.gov/business.htm].

[94] See the National Aeronautics and Space Administration's Web site at [http://www.hq.nasa.gov/office/procurement/].

so as to both assure its integrity and prevent unauthorized disclosure is also a security concern.

The General Accounting Office (GAO) has been a tenacious critic of federal electronic information security policy and practice.[95] Relying upon GAO's evaluations, Representative Stephen Horn (R-CA), chairman of the House Subcommittee on Government Management, Information, and Technology, issued a report card on federal computer security at a September 11, 2000, hearing, giving more than a quarter of the 24 major executive agencies a failing grade of F and an overall executive branch grade of D-.[96]

Remedial legislation awaits implementation. In mid-November 1999, Senator Fred Thompson (R-TN), chairman of the Committee on Governmental Affairs, with Senator Joseph Lieberman (D-CT), the committee's ranking minority member, introduced legislation (S. 1993) amending the PRA by expanding its security coverage. The report accompanying the bill when it was reported from committee on April 10, 2000, proffered the following description.

> The Government Information Security Act [S. 1993, as amended in committee] would provide a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets. It is modeled on the "best practices" of leading organizations in the area of information security. It does this by strengthening responsibilities and procedures and coordinating information policy to ensure better control and oversight of systems. It also recognizes the highly networked nature of the current Federal computing environment and provides for government-wide management and oversight of the related information security risks including coordination of security efforts between civilian, national security and law enforcement communities.[97]

The PRA, according to the committee report, would be amended in four general areas.

- *Agency Responsibilities:* Agency heads would be responsible for developing and implementing security policies. This responsibility would be delegable to the agency's Chief Information Officer or comparable official. Each agency would be responsible for developing and implementing an agency-wide security program which must

---

[95] See U.S. General Accounting Office, *Federal Information Security: Actions Needed to Address Widespread Weaknesses*, GAO Testimony GAO/T-AIMD-00-135 (Washington: Mar. 29, 2000); U.S. General Accounting Office, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO Report GAO/AIMD-00-295 (Washington: September 2000).

[96] U.S. Congress, House Committee on Government Reform, Subcommittee on Government Management, Information, and Technology, *Computer Security: How Vulnerable Are Federal Computers?*, hearing, 106th Cong., 2nd sess., Sept. 11, 2000 (Washington: transcript awaiting publication).

[97] U.S. Congress, Senate Committee on Governmental Affairs, Government Information Security Act of 1999, report to accompany S. 1993, 106th Cong., 2nd sess., S.Rept. 106-259 (Washington: GPO, 2000), pp. 1-2.

include risk assessment considering internal and external threats, risk-based policies, security awareness training for personnel, periodic reviews of the effectiveness of security policies including remedies to address deficiencies, and procedures for detecting, reporting and responding to security incidents. Further, each agency would be required to identify specific actions—including budget, staffing, and training resources—necessary to implement the security program and include this as part of its Government Performance and Results Act performance plan.

- *Director of OMB Responsibilities:* The agency plans must be affirmatively approved by the Director of OMB who also would be responsible for establishing government-wide policies for the management of programs that support the cost-effective security of Federal information systems by promoting security as an integral part of each agency's business operations. Other responsibilities of the Director would include overseeing and coordinating agency implementation of security policies, and coordinating with the National Institute for Standards and Technology on the development of standards and guidelines for security controls for Federal systems. Such standards would be voluntary and consensus-based and developed in consultation with industry. To enforce agency accountability, the Director would be authorized to take budgetary action with respect to an agency's information resources management allocations. The OMB Director may delegate these responsibilities only down to the Deputy Director for Management.

- *Annual Audit:* Based on the General Accounting Office's audit findings, S. 1993 adds a new requirement that each agency must annually undergo an independent evaluation of its information security program and practices to be conducted either by the agency's Inspector General, the General Accounting Office or an independent external auditor. GAO then will review these evaluations and report annually to Congress regarding the adequacy of agency information programs and practices.

- *National Security Systems:* S. 1993 would require that the same management framework be applied to all systems including national security systems. However, in order to ensure that national security concerns are adequately addressed and that the appropriate individuals have oversight over national security and other classified information, the [bill, as amended,] would vest responsibility for approving the security plan for these systems in the Secretary of Defense and the Director of Central Intelligence, rather than the Director of OMB. Additionally, for these systems, the Secretary of Defense or the Director of Central Intelligence shall designate who conducts the evaluation of these systems with the IG conducting an audit of the evaluation. Finally, the bill also allows the defense and intelligence

agencies to develop their own procedures for detecting, reporting and responding to security incidents.[98]

During Senate floor consideration of the Defense authorization bill for FY2001 (S. 2549) on June 19, 2000, the proposal was attached to that legislation and remained in the final version (H.R. 4205) approved by the Senate on July 13, and in the subsequent conference committee version of the legislation, which cleared Congress on October 12 and was signed by the President on October 30.[99]

Privacy. In addition to the information security considerations discussed above, federal agencies must comply with some additional requirements regarding their management—i.e., collection, use, and storage—of personally identifiable information. These are largely specified in the Privacy Act, the Computer Matching and Privacy Protection Act, and two OMB federal Web site memorandums discussed earlier in this report. The adequacy of these protections for the emerging e-government environment appears to be somewhat uncertain. For example, in the NIC survey reviewed above, only one in three (35 %) of the e-commerce users and only one in five (20 %) of the non-e-commerce users trusted that the government would keep their records confidential. These records would seemingly contain some business information, perhaps even privileged commercial information, but they would certainly contain personal information. Similarly, another public opinion survey, which was conducted for the nonpartisan, nonprofit Council for Excellence in Government and is reviewed at the end of this report, found that more than half of the respondents (55 %) were very concerned about government employees misusing personal information, and almost the same number (53 %) were concerned about the potential for less personal privacy with the onset of e-government.

Reporting on a recent survey of online privacy protections at federal Web sites, GAO found that 23 of 70 agencies had disclosed personal information gathered from their Web sites to third parties, mostly other agencies. However, at least four agencies were discovered to be sharing such information with private entities—trade organizations, bilateral development banks, product manufacturers, distributors, and retailers. The offending agencies were not identified by GAO. Responding to these findings, some privacy advocates called for updating the Privacy Act, while others urged better oversight and enforcement of the statute.[100]

When completing action on the FY2001 appropriations legislation for the Department of Transportation and related agencies, House and Senate conferees included a Web site privacy provision. Section 501 of the conference committee version of the bill (H.R. 4475) prohibits funds appropriated by the legislation to be used by any executive agency (1) to collect, review, or create any aggregate list, derived by any means, that includes the collection of any personally identifiable information relating

---

[98] Ibid., pp. 2-3.

[99] P.L. 106-398.

[100] Lance Gay, "GAO Finds Agencies Sharing Data of On-line Visitors," *Washington Times*, Sept. 8, 2000, p. A3; U.S. General Accounting Office, *Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy*, GAO Report GAO/GGD-00-191 (Washington: September 2000).

to an individual's access to, or use of, any federal government Internet site of the agency, or (2) to enter into any agreement with a third party, including another government agency, to collect, review, or obtain any aggregate list, derived from any means, that includes the collection of any personally identifiable information relating to an individual's access to or use of any nongovernmental Internet site. These limitations do not apply to any record of aggregate data that does not identify particular persons; any voluntary submission of personally identifiable information; any action taken for law enforcement, regulatory, or supervisory purposes, in accordance with applicable law; and any action that is a system security action taken by the operator of an Internet site and is necessarily incident to the rendition of the Internet site services or to the protection of the rights or property of the provider of the Internet site.[101]

The first limitation may be viewed as a response to the previously discussed June 2000 press revelation that the National Drug Control Policy Office was secretly tracking visitors to its Web site through the use of "cookies." OMB's June 22, 2000, memorandum to the heads of all executive departments and agencies indicated that "'cookies' should not be used at Federal web sites, or by contractors when operating web sites on behalf of agencies, unless, in addition to clear and conspicuous notice, the following conditions are met: a compelling need to gather the data on the site; appropriate and publicly disclosed privacy safeguards for handling of information derived from 'cookies'; and personal approval by the head of the agency." The second limitation may be regarded as a response to the September GAO report indicating that 23 agencies had disclosed personal information gathered from their Web sites to third parties. President Clinton signed the legislation into law on October 23, 2000.[102]

Two days before the President's action, press disclosures revealed that a GAO followup study contended that 13 federal agencies had ignored the OMB June 22 memorandum prohibiting the tracking of visitors to government Web sites. An appended letter from the OMB deputy director for management defended agency use of so-called "session cookies," which, the letter said, facilitate transactions at the website and are not banned by OMB. Session cookies last only as long as one is visiting the Web site. Clearly prohibited are "persistent cookies," which may track Web habits for long periods of time, and the dissemination of a person's information to a private company. GAO found seven agencies engaging in one or both of these activities.[103]

Management. In very large measure, overall management of federal executive branch e-government operations and related matters is concentrated in the leadership of OMB. The OMB director, assisted by the OIRA administrator, is vested with broad authority and responsibility for IRM by the PRA. Although the development of

---

[101] See *Congressional Record*, daily edition, vol. 146, Oct. 5, 2000, pp. H8935-H8936, H8980.

[102] P.L. 106-346.

[103] Associated Press, "U.S. Agencies Ignore Ban, Track Visitors to Web Sites," *Washington Times*, Oct. 22, 2000, p. C3; D. Ian Hopper, "Agencies Track Online Visitors Despite Rules," *Washington Post*, Oct. 22, 2000, p. A13; D. Ian Hopper, "Renewed Ban on U.S. Web 'Cookies'," *Washington Post*, Oct. 24, 2000, p. A25; U.S. General Accounting Office, *Internet Privacy: Federal Agency Use of Cookies*, GAO Letter GAO-01-147R (Washington: Oct. 20, 2000).

computer and related systems security standards for the non-military/intelligence community agencies is the responsibility of NIST, the application of and adherence to such standards by these agencies is also a responsibility assigned by the PRA to the OMB director. OMB responsibility for oversight and enforcement of agency implementation of the Privacy Act provides the OMB director with authority to address agency Web site privacy practices and uses, protection, and disposition of personally identifiable information. The Clinger-Cohen Act eliminated the primary role of the Administrator of General Services for coordinating and providing for the procurement, maintenance, and utilization of IT, and assigned to the OMB director duties for coordinating with OMB's Office of Federal Procurement Policy the development and review by the OIRA administrator of policy associated with the purchase of IT.

The Clinger-Cohen Act also mandated a CIO for each executive agency and vested this official with responsibility for carrying out the information management responsibilities assigned to the agencies by the PRA, as well as some additional duties specified in its own provisions. The CIOs were brought together in a Chief Information Officers Council established by E.O. 13011, which tasked the panel to serve as the principal interagency forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources; developing recommendations for overall federal IT management policy, procedures, and standards; sharing experiences, ideas, and promising practices, including work process redesign and the development of performance measures, to improve the management of information resources; identifying opportunities and making recommendations for, and sponsoring cooperation in, using information resources; assessing and addressing the hiring, training, classification, and professional development needs of the government with respect to IRM; and making recommendations and providing advice to appropriate executive agencies and organizations. The council is chaired by the OMB deputy director for management.

During 2000, two issues regarding CIOs came under public discussion. The first concerned the adequacy of the authority of agency CIOs to do their jobs. Some contend that public sector CIOs should have power equivalent to their private sector counterparts. For instance, with the exception of the CIOs at the Departments of Agriculture and Defense, federal CIOs do not have direct influence over information technology procurements. The federal budget process is thought to curtail exploration and adaption of new IT: private sector CIOs plan on a shorter cycle, and can take better advantage of burgeoning technology, while public sector CIOs must work in timeframes of two to five years in the future. The budget process and concomitant funding limitations also hinder government efforts to recruit and retain skilled IT professionals. Views such as these were expressed during a March 2000 hearing held by the House Subcommittee on Government Management, Information, and Technology.[104] A GAO

---

[104] U.S. Congress, House Committee on Government Reform, Subcommittee on Government Management, Information, and Technology, *The Performance of Federal CIOs: How Do They Compare with CIOs in the Private Sector*, hearing, 106th Cong., 2nd sess., Mar. 24, 2000 (Washington: transcript awaiting publication); Shrute Date, "Do CIOs Have Enough Power to Do Their Jobs?," *Government Computer News*, vol. 19, Apr. 17, 2000, pp. 1, 8.

representative testifying at this proceeding introduced a new GAO executive guide to maximizing federal CIO success by learning from private sector CIO experiences.[105]

The second issue that came under discussion was establishing a position of Chief Information Office of the United States (CIOUS) for the entire executive branch. Such an official had been proposed in 1995 Senate legislation (S. 946) underlying the Clinger-Cohen Act discussed above. A Progressive Policy Institute report recommended such a position in March 2000,[106] and legislation in support of the concept was offered in the House in June and July.[107] Texas Governor George W. Bush, the anticipated Republican presidential nominee, endorsed the CIOUS idea in a June 9, 2000, government reform speech in Philadelphia. A subcommittee hearing on the proffered bills was held on September 12.[108] Proponents of the CIOUS concept contend that many aspects of IT management would benefit from having a IT expert in charge of this area, that such an official would better facilitate OMB oversight of IT applications and use, and that efficiencies and economies could well result if this official could prevent federal agencies from purchasing computer systems that did not work or otherwise performed poorly in, or failed, security tests. Critics maintain that the CIOUS would unnecessarily perform a subset of duties currently vested in the OMB deputy director for management, would seemingly have little immediate enforcement powers, and, in some versions, might be controlling funds outside the traditional appropriations process. Members of the CIO Council reportedly are at odds over the need for the CIOUS.[109]

Maintenance. Continued maintenance of IT systems that underlie electronic government will require at least two resources: personnel and funds. Regarding the first of these resources, the CIO Council is championing the recruitment, retention, and development of IT professionals—defined as computer scientists, computer engineers, computer programmers, and systems analysts—as members of the federal civil service.

---

[105] U.S. General Accounting Office, *Executive Guide: Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, GAO Guide GAO/AIMD-00-83 (Washington: March 2000); also see U.S. General Accounting Office, *Chief Information Officers: Implementing Effective CIO Organizations*, GAO Testimony GAO/T-AIMD-00-128 (Washington: Mar. 24, 2000).

[106] See Robert D. Atkinson and Jacob Ulevich, *Digital Government: The Next Step to Reengineering the Federal Government* (Washington: Progressive Policy Institute, March 2000), p. 13.

[107] H.R. 4670 was introduced on June 15 by Rep. Jim Turner (D-TX), and H.R. 5024 was introduced on July 27 by Rep. Tom Davis (R-VA); both bills were referred to the Committee on Government Reform.

[108] U.S. Congress, House Committee on Government Reform, Subcommittee on Government Management, Information, and Technology, *Establishing a Federal CIO: Information Technology Management and Assurance Within the Federal Government*, hearing, 106th Cong., 2nd sess., Sept. 12, 2000 (Washington: transcript awaiting publication).

[109] See Christopher J. Dorobek, "Experts Debate Need for Federal IT Czar," *Government Computer News*, vol. 19, Mar. 6, 2000, p. 58; Christopher J. Dorobek, "CIO Council on Track, Members Say," *Government Computer News*, vol. 19, May 8, 2000, p. 65; Christopher J. Dorobek, "What Would Governmentwide CIO Do?," *Government Computer News*, vol. 19, July 10, 2000, p. 74; Joseph J. Petrillo, "David Bill Would Give IT Czar Carrots, but No Stick," *Government Computer News*, vol. 19, Sept. 11, 2000, p. 24.

A June 1999 council report projected that, "[w]ithin the federal government, the number of IT workers is expected to rise from 66,660 in 1997 to 71,320 by 2006. Achieving this growth," said the report, "will require replacing 32,315 and adding 4,660 new IT workers to the base." A foreseen major obstacle to recruiting such workers was "a serious disparity" in IT salary levels between the federal government and the private sector. The private sector's competing need for new and replacement IT staff was also recognized.[110] Among the recommendations offered by the report were waiving restrictions to allow federal agencies to hire skilled IT personnel retiring from the armed forces; using temporary and term appointments to speed the placement of new IT hires on the job; implementing Web-based recruiting that would allow agencies to contact potential job applicants at sites which they frequent and where timely application for employment could be made; obligating private IT contractors to perform skills transfers to government employees; and establishing a scholarship and internship program for promising IT students in exchange for government service. The Office of Personnel Management (OPM) recently announced it was creating a special pay schedule for IT workers, increasing salaries as much as 33% for entry-level and mid-level personnel, effective January 1, 2001. The increase is an attempt to make federal IT positions, which lag about $12,000, on average, behind what new hires are paid in the private sector, more competitive.[111]

However, actual practice—outsourcing—may lessen the number of federal IT employees required. According to one assessment, "more federal information technology jobs will be turned over to the private sector in coming years. The only question is whether the numbers will be modest or mammoth." In fact, the Bureau of Labor Statistics predicts a shrinking federal IT workforce, dropping from a 1998 total of 1.8 million jobs to 1.6 million in 2008—a 9% loss. The bureau also projects a rise in federal spending on IT outsourcing, increasing from $30.3 billion in 2000 to $40.3 billion in 2005. While there is agreement within the IT business sector and the federal government that IT contract employees will not eliminate their civil service counterparts, the outsourcing phenomenon will contribute to a further reduction of the federal civilian workforce in the immediate years ahead.[112]

Funds will also be needed to maintain IT systems that underlie electronic government. At a minimum, aging hardware will have to be replaced about every three to five years. More important, however, security upgrading will be necessary in order that systems can maintain operation in the face of more sophisticated cyber attacks. Reflecting this imperative, the CIO Council sent a September 6, 2000, memorandum to all Members of Congress apprising them of the need for funding essential programs for ensuring the security of the federal cyber infrastructure, and saying:

---

[110] U.S. Chief Information Officers Council, *Meeting the Federal IT Workforce Challenge* (Washington: June 1999), pp. 7-8, available from the council Web site at [http://www.cio.gov] under the heading "Documents."

[111] Stephen Barr, "Salaries for Federal Tech Workers to Increase," *Washington Post*, Nov. 4, 2000, pp. A1, A12.

[112] William Matthews, "The Outsourcing Wave Rolls On," *Federal Computer Week*, vol. 14, Sept. 25, 2000, p. 28.

> While there is significant progress, it has become clear that the foundation set of government-wide efforts to improve cyber security are hampered by a patchwork of funding and oversight structures in both the Executive and Legislative branches. In particular, efforts that are essential to providing a solid day-to-day operational foundation for cyber security across the Federal government are budgeted for by several agencies, and funding and oversight is likewise provided by a number of Congressional Committees. Federal CIO's view these programs as critical to our ability to create effective information security programs. Moreover, we are increasingly concerned that the collective visibility of these efforts is being lost. As a result, we are increasing our efforts to ensure oversight of these essential programs and to encourage budget support from Congress.[113]

By mid-October, it was apparent that several cyber security programs would not be funded, and others were in doubt as the 106th Congress moved toward final adjournment. Richard A. Clarke, Special Assistant to the President for cyber security, infrastructure protection, and counterterrorism, observed that, "because funding ... is broken up into so many different committees, no one feels they are destroying our attempt to create cyber-security."[114]

Digital Divide. As noted earlier in this report, the digital divide is a reference to the perceived disparity that results from portions of the population not having the ability to use IT due to a lack of access and/or skill. It was initially addressed by the Clinton Administration in a December 9, 1999, presidential memorandum to executive department and agency heads directing their assistance with the development of a national strategy for making computers and the Internet accessible to all Americans; expansion of the federal community technology centers network to provide low-income citizens with access to IT; encouragement of the development of IT applications that would help enable low-income citizens to start and manage their own small businesses; and use of training to upgrade the IT skills of the American workforce, particularly workers living in disadvantaged urban and rural communities. This effort was based upon assessments of the digital divide conducted by NTIA, which continue, with a view toward better understanding IT and electronic communications disparities in terms of population variables, including geography.[115]

Examination of the digital divide was also begun by the President's Information Technology Advisory Committee, which undertook an October 19, 1999, conference focusing on IT access for racial and ethnic groups in the United States. At the time the committee reported the results of this conference to President Clinton, additional conferences on geographic disparities and small university access to information tools were under consideration. The report, transmitted on February 2, 2000, urged a more coordinated national strategy for addressing the digital divide, with more community

---

[113] U.S. Federal Chief Information Officers Council, Memorandum to Members of Congress and Congressional Committee Staff, *Essential Programs for Ensuring Security of the Federal Cyber Infrastructure* (Washington: Sept. 6, 2000), p. 2.

[114] Vernon Loeb, "Cyber-Security Plans Go Begging on Hill," *Washington Post*, Oct. 16, 2000, p. A25.

[115] NTIA maintains a comprehensive *Closing the Digital Divide* clearinghouse Web site at [http://www.digitaldivide.gov].

input, greater emphasis on using IT to educate and government investment targeted toward programs to resolve the digital divide, and a market approach that better addresses issues of information inequality. The committee called for continuing research, data collection, and evaluation of the conditions contributing to the divide, and support of better IT to help increase the use of IT tools, particularly among minority owned companies, minority researchers, and policy-oriented minority employees.[116]

Emergency Response. In the American governmental experience, an expectation has long existed that the President will exert leadership when a sudden crisis threatens the nation. Such thinking may be traced to the 18th century British philosopher John Locke, who argued that occasions may arise when an executive must exert broad discretion in meeting special exigencies or "emergencies" for which the legislative authority has provided no relief and/or existing law does not grant necessary remedy. As the federal government has evolved during the past two centuries, a number of developments have occurred regarding presidential response to national emergencies, resulting in a less drastic situation than the one envisioned by Locke. Special institutions, such as the current Federal Emergency Management Agency (FEMA), have been created to respond to, coordinate the efforts of other agencies to respond to, and plan for national emergencies. Such institutions have coordinated, and contributed to, the preparation and maintenance of emergency plans, such as the Federal Response Plan for the delivery of federal disaster assistance,[117] and standby directives, such as EO. 12656 of November 18, 1988, assigning emergency preparedness responsibilities among the federal departments and agencies.[118] In addition, Congress has enacted various laws that provide the President ready authority to address an emergency, as well as some standby statutory powers that may be selectively activated under the terms of the National Emergencies Act of 1976, as amended.[119]

Responding to an emergency arising from severe disruption of computer-based critical infrastructures and e-government operations both draws upon and builds upon this legacy of developments. Experience has shown that severe weather conditions produced by a hurricane or tornado can damage or destroy communications systems and critical infrastructures in a geographic area. Consequently, the restoration of communications damaged or destroyed by severe weather is addressed in the Federal Response Plan. However, a recently added plan annex concerning terrorism indicates that the Department of Justice is responsible for "crisis management," defined as "measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism," such as damaging or destroying critical infrastructures. The annex specifies that FEMA is responsible for "consequence management," defined as "measures to protect public health and safety, restore essential

---

[116] U.S. President's Information Technology Advisory Committee, letter to the President of the United States, *Resolving the Digital Divide: Information, Access, and Opportunity* (Washington: Feb. 2, 2000), available at [http://www.ccic.gov/ac/pres-2feb00.html].

[117] The text of the Federal Response Plan is available at [http://www.fema.gov/r-n-r/frp].

[118] See *Federal Register*, vol. 53, Nov. 23, 1988, pp. 47491-47512.

[119] See 50 U.S.C. 1601 et seq.

government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism."[120]

Critical infrastructure protection planning and preparation is also addressed in PDD 63, discussed above. In addition to creating new institutions and assigning responsibilities regarding these matters, the directive establishes a public-private partnership structure, recognizing that, because "the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the government and the private sector."[121] Among the first fruits of these partnerships is the National Plan for Information Systems Protection, made public on January 7, 2000, and also discussed above.[122] An October 1999 General Accounting Office report reinforced the value of these public-private partnerships and offered various recommendations for critical infrastructure protection based upon recent experiences of addressing the year 2000 computing problem.[123]

Ultimately, in the event that severe disruption of, or damage to, critical infrastructure results in public disorder in a locale, the President may resort to the deployment of armed forces personnel, military technicians, the Ready Reserve, or federalized National Guard units to support federal law enforcement officials.[124] These troops would function under federal civilian direction; no condition of martial law would necessarily result.

Oversight. Electronic government is subject to oversight by both executive branch officials and legislative branch entities. The OMB director is a principal executive branch overseer of e-government, monitoring agency compliance with relevant statutes, presidential directives, and OMB and NIST guidance. Within departments and agencies having them, CIOs performing statutory responsibilities and duties for assuring compliance with the requirements of the PRA and monitoring the performance of IT programs also play an oversight role.[125] Also, in departments and agencies having them, Inspectors General (IG) exercise an oversight capability, particularly with regard to protecting the transmission, storage, and processing of sensitive data in electronic forms and formats.[126]

---

[120] U.S. Federal Emergency Management Agency, *Federal Response Plan* (Washington: April 1999), p. TI-1.

[121] The full text of PDD 63 is available at [http://www.fas.org/irp/offdocs/pdd/pdd-63.htm].

[122] The full text and executive summary of the national plan are available from the Critical Infrastructure Assurance Office Web site at [http://www.ciao.gov] in the "CIAO Document Library."

[123] U.S. General Account Office, *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences*, GAO Report GAO/AIMD–00-1 (Washington: October 1999).

[124] See 10 U.S.C. 332, 372, 374-375, 12301-12302, and 12406.

[125] See 40 U.S.C. 1425(c)(2) and 44 U.S.C. 3506(a)(2).

[126] See "Security, Information Technology and Facilities," *Journal of Public Inquiry*, Spring-

(continued...)

Congressional committees and subcommittees, assisted sometimes by congressional support agencies such as GAO, conduct oversight of executive entities and activities for various purposes: to ensure executive compliance with legislative intent; to improve the efficiency, effectiveness, and economy of government operations; to evaluate program performance; to investigate alleged instances of poor administration, arbitrary and capricious behavior, abuse, waste, dishonesty, and fraud; to assess agency or officials' ability to manage and carry out program objectives; to review and determine federal financial priorities; to ensure that executive policies reflect the public interest; and to protect individual rights and liberties, among other reasons.

For Congress, oversight of electronic government may prove to be particularly daunting. With potentially thousands of daily electronic transactions—for information, benefits, services, and goods—occurring, rapidly and invisibly, overseers will have to be alert to the development of administrative or managerial problems that could quickly snowball, resulting in unnecessary hardship, waste, misfeasance, or worse. Careful attention will have to be given to the creation, maintenance, preservation, security, integrity, and accessibility of the records of these transactions for possible audit and review by overseers. When agency leaders and program managers are consulted or brought before a congressional committee or subcommittee for an oversight proceeding, the agency CIO and IG may also be consulted or otherwise be found to be important participants. Moreover, for congressional and executive overseers alike, FirstGov, the single federal portal, may prove to be a useful tool for scrutinizing governmentwide compliance with certain e-government policies, such as website privacy notices, and other uniform requirements for federal Web sites.

Public Views

As the federal government embarks on the transition to e-government, early indications are that the American people are favorably inclined to many aspects of the new arrangements. A recent public opinion survey conducted for the nonpartisan, nonprofit Council for Excellence in Government found that:

- By more than a five-to-one margin (56 percent to 11 percent), the general public anticipates that the impact of e-government will be positive. Of those who described themselves as frequent Internet users, the margin was more than ten-to-one (67 percent to six percent).

- Seven in ten (71 percent) of those who visited government websites say they were impressed with the quality of the site, calling it good or excellent, and 60 percent say it was easy to find what they were looking for.

- Three in five Americans (59 percent) are opposed to voting over the Internet. Business and non-profit leaders oppose Internet voting by 57 to 39 percent and government officials oppose online voting by 49 to 39 percent.

---

[126] (...continued)
Summer 2000, pp. 28-30.

- Nearly seven in ten Americans (68 percent), including those who do not use the Internet, believe that investing tax dollars in e-government should be a priority. After being given specific examples of e-government, respondents were asked again to assess its importance. Fully 77 percent then said that investing tax dollars in e-government should be a medium to high priority.

- Even the 44 percent who said they believe that government is ineffective at solving problems and helping people, are bullish on e-government. Of this group, 51 percent predict that e-government will have a positive effect on government; and 73 percent say that investing in e-government should be a priority for tax dollars.

- Two in three Americans (65 percent) say that e-government should be developed slowly rather than quickly (30 percent) because they are concerned about security and privacy, and because many people do not have access to the Internet.

Indeed, regarding security and privacy, the survey found:

> The public's major concern about e-government is security. Two in three (66 percent) are very concerned about hackers breaking into government computers and 55 percent are very concerned about government employees misusing personal information. More than half (53 percent) are concerned about the potential for less personal privacy. Americans want government to address website security and privacy protections, and to play a role in addressing the digital divide by making sure that e-government services and information are available in other ways and that more computers are available in public spaces.

Finally, regarding the future, the survey results provided the following views.

> More than half of the general public (56 percent) and six in ten Internet users (62 percent) believe that e-government will improve the way that government operates. Only one in ten Americans (11 percent) believes the impact of e-government will be negative. Ninety-two percent of government officials and three in four business and non-profit leaders (76 percent) also believe e-government will improve government operations.[127]

Related CRS reports and issue briefs following legislation pertaining to the e-government components discussed above are identified in the reading list at the end of this report.

---

[127] Conducted by the research firms of Peter D. Hart and Robert M. Teeter, the study surveyed 150 government officials, 155 business and non-profit leaders, and 1,003 members of the general public during Aug. 14-16, 2000. Quotations cited above appear in the Council's Sept. 28 press release summarizing the results of the study. This press release and the full study report are available from the Council's Web site at [http://www.excelgov.org].

Glossary

APA	Administrative Procedure Act
CIO	chief information officer
CIOUS	Chief Information Officer of the United States
COPPA	Children's Online Privacy Protection Act
DOD	Department of Defense
E-commerce	electronic commerce
E-FOIA	Electronic Freedom of Information Amendments
FEMA	Federal Emergency Management Agency
FirstGov	the single federal portal to all national government Web sites
FOIA	Freedom of Information Act
GAO	General Accounting Office
GPEA	Government Paperwork Elimination Act
HUD	Department of Housing and Urban Development
IG	Inspectors General
IRM	information resources management - the planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by agencies
IT	information technology
IT2	Technology for the 21st Century initiative announced by the President on January 24, 1999
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
OIRA	Office of Information and Regulatory Affairs
OMB	Office of Management and Budget
OPM	Office of Personnel Management

PDD	Presidential Decision Directive
PRA	Paperwork Reduction Act
USPS	United States Postal Service

For Further Reading

CRS Documents

CRS Report 98-675, *Critical Infrastructures: A Primer*, by John D. Moteff.

CRS Report RL30153, *Critical Infrastructures: Background and Early Implementation of PDD-63*, by John D. Moteff.

CRS Issue Brief IB96039, *Encryption Technology: Congressional Issues*, by Richard M. Nunno.

CRS Report RS20426, *Electronic Commerce: An Introduction*, by Glenn J. McLoughlin.

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

CRS Report 98-845, *Federal Government Information Technology Policy: Selected Issues*, by Glenn J. McLoughlin et al.

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

CRS Report RL30719, *Internet Access—Broadband and the Digital Divide: Federal Assistance Programs*, by Lennard G. Kruger.

CRS Report 98-67, *Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth*, by Marcia S. Smith, Richard M. Nunno, John D. Moteff, and Lennard G. Kruger.

CRS Report RS20035, *Internet Privacy—Protecting Personal Information: Overview and Pending Legislation*, by Marcia S. Smith.

CRS Report RL30322, *Online Privacy Protection: Issues and Developments*, by Gina Marie Stevens.

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

CRS Report RL30671, *Personal Privacy Protection: The Legislative Response*, by Harold C. Relyea.

CRS Report 98-649, *Spinning the Web: the History and Infrastructure of the Internet*, by Rita Tehan.

Other Documents

Council for Excellence in Government, *E-Government: The Next American Revolution*, by Hart-Teeter (Washington: September 2000), available at [http://www.excelgov.org].

National Research Council, *Improving Surface Transportation Security* (Washington: National Academy Press, 1999).

National Research Council, *Information Technology Research for Crisis Management* (Washington: National Academy Press, 1999).

NIC, *Benchmarking the eGovernment Revolution: Year 2000 Report on Citizen and Business Demand*, by the Momentum Research Group of Cunningham Communication (Reston, VA: NIC, 2000).

Office of the Vice President, *Access America: Reengineering Through Information Technology, Report of the National Performance Review and the Government Information Technology Services Board* (Washington: GPO, 1997).

Stiglitz, Joseph E., Peter R. Orszag, and Jonathan M. Oszag, *The Role of Government in a Digital Age*, commissioned by the Computer and Communications Industry Association (Washington: October 2000), available at [http://www.ccianet.org/digitalgovstudy/main.html].