HEINONLINE

Citation: 7 Bernard D. Reams Jr. Law of E-SIGN A Legislative of the Electronic Signatures in Global and National Act Public Law No. 106-229 2000 iii 2002

Content downloaded/printed from HeinOnline (http://heinonline.org) Sun Apr 21 23:18:13 2013

-- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at http://heinonline.org/HOL/License

-- The search text of this PDF is generated from uncorrected OCR text.

98-845 STM

CRS Report for Congress

Federal Government Information Technology Policy: Selected Issues

Updated January 5, 1999

Glenn J. McLoughlin, Coordinator
Specialist in Technology and Telecommunications Policy
Science, Technology, and Medicine Division



Congressional Research Service • The Library of Congress

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [iii] 2002

ABSTRACT

This report provides an overarching review of current federal government information technology (IT) policy issues. The issues selected for this report are federal government IT spending, the year 2000 problem, encryption policies, information infrastructure and national security, the Government Performance Results Act (GPRA), the Clinger-Cohen Act, medical records and privacy, electronic commerce, domain names, and the federal role in the current and future development of the Internet. The report provides concise summaries of these issues. At the end of each section, a short list of relevant and more detailed CRS reports on the subject is provided. This report will be updated periodically.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [iv] 2002

Federal Government Information Technology Policy: Selected Issues

Summary

Federal government information technology (IT) is an important part of the federal mission to serve Americans. Federal government IT policy can improve how services and information are provided to citizens, increase the timeliness and quality of federal agencies' responses, and save federal tax dollars by improving government efficiency. Protection and security of individuals' privacy, as well as making appropriate federal data more transparent and available for its citizens, are the ultimate goals of federal agency IT policies.

But there are some questions and concerns regarding federal IT policy as well. Are the programs that support federal policy appropriately funded and administered? Is enough being done to safeguard and protect citizens from both immediate and long-term threats? What is the proper federal role for enhancing all forms of IT applications and development? Federal policymakers grapple with these questions and others as they consider establishing, reviewing, and sometimes revising the federal government's IT policy.

Among the many federal IT policy issues now before congressional policymakers, the following are likely to continue to receive attention. They are: the size and scope of federal government IT spending, the year 2000 computer problem, federal encryption policies, information infrastructure and national security, implementation of both the Government Performance and Results Act (GPRA) and the Clinger-Cohen Act, the role of the federal government with regard to medical records and privacy, electronic commerce, domain names, and the federal role in the growth and the future of the Internet. This report provides a brief summary of each issue, and lists more detailed CRS reports after each section.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [v] 2002

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [vi] 2002

Contents

Overview 1
- Federal Government IT Spending 2
- The Year 2000 Computer Problem 3
- Encryption Policies 5
- Information Infrastructure and National Security 7
- The Government Performance and Results Act (GPRA) 10
- The Clinger-Cohen Act 12
- Medical Records and Privacy 14
- Domain Names 16
- Electronic Commerce 19
- The Internet and the Federal Role 21

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [vii] 2002

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [viii] 2002

Federal Government Information Technology Policy: Selected Issues

Overview

The 105th Congress addressed a wide range of information technology related issues, from privacy and security to commerce and taxation, and from the federal role in funding and developing the Internet to the private sector role in advancing new technologies and applications. Since some of these issues are still unreconciled, it is likely that the 106th Congress will continue to address a wide range of IT issues, many directly connected to federal IT policies and programs.

Federal IT policy, and the programs that support the policy, can have a wide range of benefits for U.S. citizens. Federal government IT policy can improve how services and information are provided to Americans, increase the timeliness and quality of federal agencies' responses, and save federal tax dollars by improving government efficiency. Those are all reasons why the federal government increasingly relies on IT applications and services. Protection and security of individuals' privacy, as well as making appropriate federal data more transparent and available for its citizens, are the ultimate goals of federal agency IT policies.

Many have questions and concerns regarding federal IT policy as well. They view the rapidly expanding types of IT technologies, and the many applications of these technologies and ask: are the programs that support federal policy appropriate? Is enough being done to safeguard and protect citizens from both immediate and long-term threats? What is the proper federal role for enhancing all forms of IT applications and development?

It is important to remember that just over two decades ago, federal government IT policy usually meant the acquisition and use of one mainframe computer per federal agency. The number of qualified professionals who could use and maintain mainframe databases was relatively small. The subsequent mushrooming of new technologies and applications has ranged from the omnipresent use of personal computers in the federal workplace to the explosive growth of the Internet. Often, federal policymakers have had to react to these changes as they attempt to fit new IT technologies and applications into existing policy frameworks. The following summaries of current federal IT policy issues provide a broad view of how the federal government is addressing many of these changes.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 1 2002

Federal Government IT Spending[1]

The federal government has a significant presence in the U.S. information technology (IT) industry. Since traditionally, federal government procurement and acquisition is standardized, its buying patterns can shape and determine specific technology developments and applications in IT. As a single buyer, federal agency IT procurement in the 1960s and 1970s helped spur the growth of the U.S. computer and semiconductor industries, and provided a significant impact on U.S. computer software and networking capabilities, and peripheral services. Even after a 1996 law (P.L.104-106) decentralized much of the federal government IT procurement and acquisition, the federal government, if considered as a single entity, is still one of the single largest buyers of IT services and technologies in the world.

Until the 1996 law, federal IT procurement and acquisition for most federal agencies was centrally managed by the General Services Administration (GSA), and statistics on federal IT procurement and use came from one source. Since 1997, as authority has become more decentralized at individual agencies, there has been less centralized reporting of total federal information technology. However, some figures are available from the Office of Management and Budget (OMB) on federal IT procurement and acquisition.

OMB figures show that IT expenditures make up a small portion of the overall federal operating budget (6% in FY1996). Over the last two fiscal years, federal IT spending was relatively flat, growing 2% from $28.6 billion in FY1997 to $29.1 billion in FY1998. Hardware budgets totaled $5 billion in FY1998, slightly above FY1997 budgets. Software budgets declined marginally in the FY1998 budget to $1.4 billion from just less than $1.5 billion in FY1997. In contrast, U.S. business spent just under $400 billion on IT technologies and services in calendar year 1997, 88% of all IT technologies and services purchased in the United States.

The most significant change in the FY 1998 budget is an increase in commercial services, where the federal government is contracting out more and more of its IT systems and services. According to a November 1997 report by Input, a private sector firm, federal market demand for vendor-furnished information systems and services will increase from $22.6 billion in FY 1997 to $30.1 billion in FY 2002 at a compound annual growth rate of 5.9%. Another IT industry report, by Federal Sources, Inc., provides the result of an annual survey of large companies doing business in the federal IT field. The current report forecasts 8% growth in federal IT spending in FY1998, and an increase from just less than $30 billion in FY1998 to $40 billion by FY2002.

According to a General Accounting Office (GAO) report issued in June 1997, the federal government spent $349 million on Internet-related activities over a three-year period (*Internet and Electronic Dial-Up Bulletin Boards: Information Reported by Federal Organizations*, GAO/GGD-97-86). The Defense Department was

---

[1]Prepared by Rita Tehan, Information Research Specialist, Congressional Reference Division and Glenn J. McLoughlin, Specialist in Technology and Telecommunications Policy, Science, Technology, and Medicine Division.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 2 2002

responsible for the bulk of the spending, but Internet spending and usage vary widely across the government. Of the major agencies, Veterans Affairs spent the least ($1.9 million over three years) and the Department of Defense spent the most ($147.8 million) over the same period of time. (The State Department did not respond to GAO's survey). During this period, nearly one-third of federal employees were hooked up to the Internet, while 1.7 million federal workers (about 50 percent) had email access, but online access varied by agency.

See also:

Brad Meyers, *Computer Almanac: Interesting and Useful Numbers About Computers*. [http://www.cs.cmu.edu/afs/cs/user/bam/www/numbers.html]

The Year 2000 Computer Problem[2]

Many computers in the United States and throughout the world will not be able to store or process dates correctly beyond December 31, 1999 unless they are modified. The problem is the result of a common computer design in which dates are stored using only the last two digits for the year (e.g., 98 for 1998). The two-digit "year field" is very common among older systems designed when memory storage was more expensive, but is also used in many systems built recently. Under the two-digit format for storing the year, the year 2000 is indistinguishable from 1900. The year field in computer programs can perform various functions such as calculating age, sorting information by date, and comparing dates. When years beyond 1999 are entered in the two-digit format, those functions will often fail to operate properly, and in some cases systems will completely shut down. Although the year 2000 problem is primarily in computer software, the problem also exists in some hardware components in which integrated circuits, also called embedded chips, store or process data. Without correction, computer malfunctions will cause many costly problems in commerce and government.

Although some may still doubt the seriousness of the problem, most government officials and business managers are now convinced that tending to it is critically important to continue operations. Fixing computer systems for the year 2000 will, in general, be very difficult and costly due to the large number of computers in use, their high degree of interdependence, and the difficulty in finding all of the date fields in the software. All of the year 2000 conversion work, including testing for errors and testing interfaces between systems, must be completed before January 1, 2000 to avoid disruptions in a system. In addition, many report a shortage of skilled programmers to perform the year 2000 conversion.

Over 50 GAO reports have concluded that many federal agencies are at risk of failing to complete the year 2000 conversions of their mission critical systems by the deadline. The GAO has identified specific systems that are at greatest risk and has made recommendations to agencies to mitigate failures. Federal agencies are all working to renovate their systems, and a Presidential Council on Year 2000

---

[2]Prepared by Richard M. Nunno, Analyst in Information Technology, Science, Technology, and Medicine Division.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 3 2002

Conversion has been established to oversee activities in federal agencies, and coordinate with state, local, and tribal governments, international groups and the private sector on all year 2000 conversion efforts. An interagency committee has recommended that a four-digit year field be used for all federal electronic data exchange, and has required federal agencies to purchase systems that process all dates correctly.

The Office of Management and Budget has been submitting quarterly reports to Congress on the status of federal agency year 2000 conversion. The OMB report, dated as of August 15, 1998, identifies the following agencies as not making satisfactory progress: the Departments of Defense (DOD), Education, Energy, Health and Human Services (HHS), Transportation, State, and the Agency for International Development. Critical government services as well as military operations face possible risks to their ability to continue to function properly. According to OMB's estimates, the cost of year 2000 conversion for all federal agencies has continued to increase, their most recent estimate being $5.4 billion.

State and local governments, private sector businesses, and foreign organizations also face the year 2000 problem for their computer systems, which could have an impact on international trade and the overall economy. Interconnected systems must also be protected from receiving corrupted data from systems that are not year 2000 compliant. Several economic sectors considered critical to the nation also face risks of experiencing year 2000 failures. These include utilities and the national power grid, telecommunications, banking and financial services, health care services, transportation services, agriculture and food processing and distribution, and small businesses.

Many congressional hearings have been held from 1996 to the present, raising the level of awareness of the year 2000 problem at all levels in government agencies and the private sector. Several appropriations bills enacted in the 104th and 105th Congresses have contained year 2000 provisions. Three FY1998 Appropriations Acts direct the reprogramming of funds from existing appropriations of federal agencies to perform year 2000 work. (P.L. 105-61, P.L. 105-65, P.L. 105-78). An FY1998 Supplemental Appropriations Act (P.L. 105-174) provides new funding for year 2000 efforts at federal agencies.

Emergency year 2000 funding for federal agency conversion efforts (totaling $3.85 billion) was enacted as part of the FY1999 Omnibis Appropriations Act (P.L. 105-277). Of this funding, $1.1 billion is directed specifically for DOD. The remaining $2.5 billion is to be distributed by OMB to other federal agencies (except for approximately $30 million which is directed to the legislative and judiciary branches). OMB has already approved allocations of $891 million for non-defense agency use. For DOD, the Defense Authorization Act for FY1999 (P.L. 105-261) contains directions for managing its year 2000 conversion efforts. All of these emergency federal funds will remain available until September 1, 2001, and may be used only for federal year 2000 remediation, unless otherwise directed by Congress.

One year 2000 bill that was not part of an appropriations bill was enacted in the 105th Congress. That bill, the Examination Parity and Year 2000 Readiness for Financial Institutions Act (P.L. 105-164), extends the authority of the Office of Thrift

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 4 2002

Supervision and the National Credit Union Administration to examine the operations of service corporations or other entities that provide computer maintenance and data processing services for thrift savings institutions and credit unions. The legislation was intended to give those federal agencies statutory parity with other financial regulatory agencies for the financial institutions they oversee.

Policymakers also have been concerned about making it easier for companies to disclose information on the year 2000 readiness of their products and services. The Year 2000 Information and Readiness and Disclosure Act (P.L. 105-271) was enacted to encourage companies to disclose information on the status of the year 2000 renovations and testing of their products and services. To protect companies, the Act prohibits "year 2000 readiness disclosures" from being used as evidence in state or federal courts. It also protects companies from "year 2000 statements" in liability suits, unless the statement is known to be false, intended to deceive, or made in reckless disregard for truthfulness. It also exempts from federal antitrust action information sharing by companies of year 2000 remediation activities.

The 106th Congress will likely hold hearings to monitor federal agency progress of year 2000 remediation. Congress will likely also seek to assist state and local governments, the private sector, and global information systems vulnerable to the year 2000 problem. Policymakers may consider additional legislation that would be intended to remove obstacles for completing year 2000 conversion in each of these sectors.

See also:

Richard M. Nunno, *The Year 2000 Problem: Activity in the 105th Congress.* CRS Issue Brief 97036. Updated regularly.

Richard M. Nunno, *Year 2000 Problem: Chronology of Legislation.* CRS Report 98-377. 5 August 1998.

Encryption Policies [3]

Encryption and decryption are methods of using cryptography to protect the confidentiality of data and communications. When encrypted, a message only can be understood by someone with the key to decrypt it. Businesses and consumers want strong encryption products to protect their information, while the Clinton Administration wants to ensure the law enforcement community's ability to monitor undesirable activity in the digital age. The Administration's policy promotes the use of strong encryption, here and abroad, as long as it is designed with "key recovery" features where a "key recovery agent" holds a "spare key" to decrypt the information. The Administration would require key recovery agents to make the decryption key available to duly authorized federal and state government entities. Privacy advocates are concerned that law enforcement entities will have too much access to private information.

---

[3]Prepared by Richard M. Nunno, Analyst in Information Technology, Science, Technology, and Medicine Division.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 5 2002

Encrypting messages so they can be understood only by the intended recipient historically was the province of those protecting military secrets. The burgeoning use of computers and computer networks, including the Internet, now has focused attention on its value to a much broader segment of society. Government agencies seeking to protect data stored in their databases, businesses wanting to guard proprietary data, and consumers expecting electronic mail to be as private as first class mail, all want access to strong encryption products. While encryption is uncommon for telephone users today, the advent of digital telephone services (particularly Personal Communication Services, PCS, a digital form of cellular telephony) is expected to make encrypted voice and data communications over telephones more common.

The National Institute of Standards and Technology (NIST), in conjunction with industry, developed an encryption standard using a 56-bit key in 1977. Called the Data Encryption Standard (DES), it is widely used today in the United States and abroad. NIST is currently working to establish a new, stronger standard than DES referred to as the Advanced Encryption Standard (AES). The need for a stronger standard was underscored in June 1997 when DES was broken.

The Administration uses the export control process to influence whether companies develop key recovery encryption products by making it easy to export products with key recovery, and difficult for those products without. There are no limits on domestic use or import of any type of encryption. The Clinton Administration has tried to influence what is available for domestic use through export controls, since most companies will not develop one product for domestic use and a separate product for export. U.S. computer companies argue that U.S. export restrictions hurt their market share, and help foreign companies that are not subject to export restrictions. Many businesses and consumer groups agree that key recovery is desirable when keys are lost, stolen, or corrupted. However, they would like market forces—not government directives—to drive the development of key recovery encryption products. Many also object to government having any role in determining who can hold the keys.

All parties agree that encryption is essential to the growth of electronic commerce and use of the Internet, but there is little consensus beyond that. Seven bills on encryption or computer security have been introduced in the 105th Congress. Fundamentally, the controversy over encryption concerns what access the government should have to encrypted stored computer data or electronic communications (voice and data, wired and wireless) for law enforcement purposes. Among the major issues facing congressional policymakers are the following.

- **Key Recovery.** The Clinton Administration wants law enforcement access to keys for encrypted data stored by computers, transmitted between computers, or other types of electronic communications. Not only does the Administration view this as critical for U.S. users, but it seeks creation of a global key management infrastructure (KMI) to ensure confidentiality for the growth of global electronic commerce, and monitoring undesirable activity (by terrorists, drug cartels, or child pornographers, for example). Some contend that market forces will drive the development of a KMI for stored computer data without government involvement. Others have concerns that the government will have

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 6 2002

unfettered entry to private files and communications. In September 1998, the Administration announced a new encryption policy that will allow companies to export 56-bit encryption products without demonstrating they have plans for creating or developing key recovery systems.

- **Export Restrictions.** The Clinton Administration, defending its export control policy, points to threats to national security and public safety that would arise if criminals and terrorists used encryption that the U.S. government could not decrypt. Opponents of the Administration's policy counter that the United States cannot prevent access to strong non-key recovery encryption by criminals and terrorists, because it is already available elsewhere in the world. They argue that the current policy of no restrictions on domestic use or import of encryption means that domestic threats likely would not be affected. In July 1998, the Administration announced plans to relax export controls for strong encryption software without requiring provisions for key recovery for financial institutions in the 45 countries that currently have laws acceptable to the United States outlawing money laundering. The Administration's new policy, announced in September 1998, expands the export of 56-bit encryption to insurance companies, health and medical organizations (excluding biomedical and pharmaceutical manufacturers), and on-line merchants for client server applications that secure electronic commerce transactions. Some in industry and Congress question whether the Administration's policy, since many no longer consider 56-bit encryption a strong encryption method.

- **Domestic Use.** Current U.S. policy allows any type of encryption to be used in or imported into the United States. Administration concerns that attempting to change this policy would be unsuccessful was a factor in its choice of using export controls to influence what encryption products are available for domestic use. In 1997, some experts detected a change in government policy when FBI Director Freeh informed the Senate Judiciary Committee of the possibility of requiring that key recovery be built into products manufactured in or imported into the United States. Key recovery could possibly be enabled by the manufacturer, not only the user. Congressional policymakers will likely revisit, and pursue, this issue with the Clinton Administration.

See also:

Richard M. Nunno, *Encryption Technology: Congressional Issues.* CRS Issue Brief 96039. Updated regularly.

Information Infrastructure and National Security [4]

Information technology pervades many, if not most, of the systems used to create and distribute the many public and private services upon which our society now depends (from deploying and operating military units to providing local 911 service).

---

[4]Prepared by John D. Moteff, Specialist in Science and Technology Policy, Science, Technology, and Medicine Division.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 7 2002

These systems, or infrastructures, are becoming more interdependent by the increased use of telecommunications that link the information technology of one system with those of others. National security, defined in the broadest sense to include not only military security and defense capability, but also economic security and social cohesion, increasingly depends on the integrity of the information technology operating and managing those systems and the connections between them.

The country has typically thought of the integrity of its infrastructure in terms of the physical vulnerability to natural forces (e.g., earthquakes) and to man-made threats (e.g., sabotage). But the security community also is concerned about the electronic vulnerability of its infrastructure, or more specifically the data and the software used by these systems. Electronic threats, too, can be natural or man-made. Of particular interest is the man-made threat posed by "hackers" who might enter the information infrastructure of a particular system and corrupt it. In the past "hackers" may have been inquisitive or mischievous individuals motivated by the challenge of breaking into the information infrastructure of an organization. Today, there is concern that "hackers" may include groups of individuals working toward more nefarious ends. While the public and the private sectors have long been worried about spies "hacking" into sensitive information, the concern now is that "hackers" may soon represent the vanguard of a hostile attack by foreign entities in a way that is difficult to detect. This issue was raised during a four day conference on national information systems security, October 5-8, 1998, sponsored by the National Institute of Standards and the National Security Agency's National Computer Security Center.

Individually, system operators have spent varying amounts of time and resources protecting and policing their information systems. The telecommunications industry and the military and emergency preparedness communities have cooperated for years to assure the integrity of the nation's civil and military telecommunication systems (90% of the military's communications travel on the civilian system) against both physical and electronic threats. But, as telecommunications link the information infrastructure of various other systems, and as a disruption in one system can lead to cascading disruptions in other systems, the national security community would like to expand that cooperation to other sectors of the economy.

In July 1996, the President established (through Executive Order 13010) the President's Commission on Critical Infrastructure Protection (PCCIP). Among its tasks, the Commission was to: a) assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures; b) determine what legal and policy issues are raised by efforts to protect critical infrastructures; c) recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures, and d) propose any statutory or regulatory changes necessary to effect its recommendations. The Commission examined the following systems— information and communication; energy (including electrical power, gas and oil); banking and finance; physical distribution (personal and commercial road, rail, and air transport); and vital human services (including water, local emergency services, and federal services such as weather, disease control, and social security)—concentrating on the electronic vulnerabilities and threats.

In October 1997, the Commission released an unclassified report (*Critical Foundations: Protecting America's Infrastructures*). Generally, while the

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 8 2002

Commission did not find any immediate threat, it did report that the critical infrastructures examined were vulnerable to attack with tools now available. There were several specific findings. They include: information sharing is the most immediate need (currently there is no comprehensive body of knowledge available for effective analysis of overall vulnerability and threats), responsibility for protecting and responding is shared among owners and operators and the government, the capabilities and response of diverse federal agencies need to be coordinated, adequate response must occur in changing environments, the federal government should lead by protecting its own systems, the legal framework is imperfectly attuned to deal with electronic threats, and research and development is presently inadequate to support protection.

Among its recommendations, the Commission suggested the establishment of a national structure for assuring the integrity of critical infrastructures. Such a structure would include a set of councils and offices meant to bring together various stakeholders to share information, and develop protection strategies and responses. The Commission also recommended that among the laws that should be reviewed are the Defense Production Act, the Stafford Act/Federal Response Plan, the Nunn-Lugar-Domenici program (which focuses federal resource on training and access to equipment for local first responders) and criminal statutes. The Commission estimated that the federal government spends about $250 million a year on research and development to protect its infrastructure (about $150 million of which goes toward protection of information systems). The Commission recommended that the investment be doubled in 1998 and increased to $1 billion a year for the next 5 years.

On February 27, 1998, the Department of Justice announced the creation of the National Infrastructure Protection Center (NIPC). Its mandate is to detect, prevent and respond to cyber and physical attacks on U.S. computer systems. The Center has links to other government departments such as Defense, State, and Treasury, as well as to local and international police agencies. On May 22, 1998, President Clinton signed Presidential Directive 63. It expands the FBI's authority to operate the NIPC and to facilitate and coordinate the federal government's response to any incident, and to investigate threats. The center also serves as a clearinghouse for information shared among agencies and with the private sector. The Commerce Department has been named the lead agency for overseeing an information and communications center. Each federal agency will be in charge of protecting its own critical infrastructure, particularly its electronic systems, and must develop a critical infrastructure protection plan.

See also:

John D. Moteff, *Critical Infrastructures: A Primer*. CRS Report 98-675. 13 August 1998.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 9 2002

The Government Performance and Results Act (GPRA) [5]

The Government Performance and Results Act (GPRA or "The Results Act"), was enacted in 1993 as P.L. 103-62. One of the key purposes of GPRA is to improve congressional decision making by providing more objective information on the relative effectiveness and efficiency of federal programs and spending. The Act essentially mandates strategic planning and performance measurement in the federal government. P.L. 103-62 requires federal agencies to develop strategic plans describing their overall goals and objectives, annual performance plans containing quantifiable measures of their progress, and performance reports describing their success in meeting those standards and measures.

Each agency's strategic plan is required to contain the following elements: a comprehensive mission statement covering the major functions and operations of the agency; general goals and objectives, including outcome-related goals and objectives, for the major functions and operations of the agency; a description of how the goals and objectives are to be achieved, including a description of the operational processes, skills and technology, and the human capital, information, and other resources required to meet those goals and objectives; a description of how the performance goals included in the agency's annual performance plan are related to the general goals and objectives in the strategic plan; an identification of those key factors external to the agency and beyond its control that could significantly affect the achievement of the general goals and objectives; and a description of the program evaluations used in establishing or revising general goals and objectives, with a schedule for future program evaluations.

Performance plans are prepared in conjunction with an agency's annual budget submission to Congress. The performance plan should establish a tangible link between the long term strategic goals presented in the strategic plan, and an agency's program activities. P.L. 103-62 requires agency performance plans to: establish performance goals to define the level of performance to be achieved by a program activity; express such goals in an objective, quantifiable, and measurable form; briefly describe the operational processes, skills and technology, and the human, capital, information, or other resources required to meet the performance goals; establish performance indicators to be used in measuring or assessing the relevant outputs, service levels, and outcomes of each program activity; provide a basis for comparing actual program results with the established performance goals; and describe the means to be used to verify and validate measured values. In cases where performance goals for a program activity cannot be expressed in an objective, quantifiable, and measurable form, the agency may, with OMB approval, express performance goals by using descriptive statements or other appropriate alternate forms.

Performance reports will discuss the extent to which performance goals and objectives are met. Strategic plans were submitted to Congress and OMB on September 30, 1997, and are required to be updated at least once every three years. Agency performance plans were submitted in early 1998 in conjunction with FY1999

---

[5]Prepared by Lennard G. Kruger, Specialist in Science and Technology, Science, Technology, and Medicine Division.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 10 2002

budget submissions. Performance reports will be released annually, starting in March 2000. Each of these plans and reports are to be shared with Congress, which is expected to use the materials to help guide budgetary decisions.

While P.L. 103-62 does not directly address federal information technology, IT can be expected to play a key role in determining whether agencies can successfully implement GPRA. In many cases, the ability of agencies to collect and measure program performance data, and to verify and validate results, will depend on efficient and effective IT systems. In its review of agency strategic plans (*Managing for Results: Critical Issues for Improving Federal agencies' Strategic Plans*, GAO/GGD-97-180), GAO concludes that information gathering is a major obstacle to GPRA implementation. The GAO suggests that "the questionable capacity of many agencies to gather performance information has hampered, and may continue to hamper, efforts to identify appropriate goals and confidently assess performance."

Not surprisingly, information systems become a critical factor in enabling agencies to effectively implement GPRA. Without reliable IT systems, says GAO, "agencies will not be able to gather and analyze the information they need to measure their performance, as required by the Results Act." Yet despite the criticality of IT systems, GAO determined that most of the 27 agency strategic plans "did not cover strategies for improving the information management needed to achieve their strategic goals." The plans provided few details on how agencies plan to upgrade or utilize their IT systems in order to better gather and measure performance data. In parrticular, GAO cites OPM's failure to discuss year 2000 despite the fact that "many of its critical information systems are date dependent and exchange information with virtually every federal agency." The GAO also criticizes DOD's plan which "did not specifically address information security even though DOD recognizes that information warfare capability is one of a number of areas of particular concern, especially as it involves vulnerabilities that could be exploited by potential opponents of the United States."

Finally, says GAO, in order to ensure that federal IT systems can adequately support GPRA implementation, it is important for agencies to follow through with implementation of the Chief Financial Officers Act (P.L. 101-576), the Clinger-Cohen Act (P.L. 104-106), and the Paperwork Reduction Act (P.L. 104-13). Indeed, GPRA can be viewed as part of the statutory framework put in place during the 1990s to address weaknesses in the management of federal programs, including IT-related programs. In particular, the Clinger-Cohen Act requires agencies to consider how information systems will help them carry out their missions and the performance they can expect from those investments. Ultimately, the success or failure of federal IT initiatives is likely to be viewed not only within the context of the Clinger-Cohen Act, but also within the context of GPRA and the extent to which agencies meet their overall strategic goals and performance standards.

See also:

Genevieve J. Knezo, *Government Performance and Results Act: Implementation and Issues of Possible Concern.* CRS Report 97-1028. 14 July 1998.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 11 2002

Frederick M. Kaiser and Virginia A. McMurtry, *Government Performance and Results Act: Implications for Congressional Oversight.* CRS Report 97-382. 12 May 1997.

The Clinger-Cohen Act [6]

Federal information technology procurement and financial management policies are an increasingly important part of the way the federal government conducts its business. Since the late 1980s, reform of federal IT procurement and acquisition policies has been part of congressional debate. Reform was rooted in changing or repealing the 1965 Automatic Data Processing Act, or, as it was more popularly known, the Brooks Act. The Brooks Act was intended to address problems of passive, partial, or informal types of leadership in the purchasing, leasing, maintenance, operation, and utilization of automatic data processing (ADP) by federal agencies. Federal agencies had reported that they were having difficulty complying with regulations for annual agency-wide ADP budget reviews. The Brooks Act was intended to centralize and coordinate this process by giving the General Services Administration (GSA) operational responsibility for ADP management, utilization, and acquisition.

Over the past three decades, however, advances in information technology and applications created a new environment for federal agencies. Many viewed the Brooks Act as causing procurement delays, imposing "one size fits all" standardized technology solutions, and mismatching technology solutions with agencies' missions. Policymakers sought to redress these problems and reform the centralized federal acquisition, procurement, and financial accounting system. The Clinger-Cohen Act, or as it was passed, the Information Technology Management Reform Act, was incorporated into the National Defense Authorization Act for Fiscal Year 1996 (P.L. 104-106). The Clinger-Cohen Act (named after its principal co-sponsors) was intended to provide the executive branch flexibility to acquire technologies and services incrementally, enter into modular rather than more costly longer-term contracts, and obtain information technologies and services to fit agency needs.

The major provisions of the Clinger-Cohen Act are the following.

- It eliminated GSA's central role for setting information technology policy and provided each federal agency with direct responsibility for IT procurement and acquisition.
- It mandated that each federal agency establish a Chief Information Officer (CIO) to provide administrative and managerial oversight of each agency's IT policies.
- It established two types of pilot programs for federal agency IT management and procurement.

---

[6]Prepared by Glenn J. McLoughlin, Specialist in Technology and Telecommunications Policy, Science, Technology, and Medicine Division.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 12 2002

- It gave OMB a broad role in coordinating and facilitating interagency IT communication on policies.

To date, many in government and the private sector are encouraged that the Act's provisions have provided overall cost reductions for the federal government. Many contend that the law has greatly improved the efficiency of individual agencies as information technology purchases and applications are more tailored to each agency's need and mission. The long-term savings to the federal government could be significant. Yet, wide-ranging federal information technology reform is still relatively uncharted territory. Supporters also contend that the law's provisions, based on successfully proven private sector initiatives, also have decentralized and reduced the bureaucracy inherent in federal information technology management policy, and will likely result in improved federal services in the near future. Supporters also contend that the creation of federal agency CIOs and the nascent pilot programs will provide federal agencies with the expertise and the procedures for evaluating success and failure. Several federal agencies have made significant inroads in changing federal information management through their CIO offices.

Yet it is unclear whether a total dollar figure in savings can be determined under this law. Some are concerned that, because federal agencies may be too focused on serving their own needs and missions, standardized information technologies, applications, and services may be lacking across the government. They are not convinced that federal agencies will derive all of the benefits supporters claim. They argue that such benefits, adopted from the private sector, may not necessarily work where the mission is the public good, not profit. What policies will guide federal information technology managers use when forceful marketplace mechanisms such as profit and loss are not available to purge failure?

Finally, some contend that simply providing for CIOs and pilot programs will not solve (or perhaps even address) the fundamental issue of developing good and responsive government. Can the Clinger-Cohen Act live up to expectations that government reforms will produce better services? Some experts contend that, without talented personnel, federal information resources management (IRM) will not fully benefit from the Act. Some even state that the federal government is so far behind the private sector in attracting and keeping IRM expertise that no amount of reform will reverse this trend. According to an expert at the GAO, federal agencies are not identifying the skills they need and they can not afford to pay for the skills they need. Yet, supporters are optimistic that the Clinger-Cohen Act may create an environment where bright and skillful people are challenged by the flexibility and responsiveness arising from the law. Many hope that the Act will usher in a new age in which the best and the brightest in IRM will enter the government and serve the public good.

See also:

Glenn J. McLoughlin, *Information Technology Management Reform Act (ITMRA) of 1996.* CRS Report 97-79. 8 January 1997.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 13 2002

Medical Records and Privacy [7]

The ability to ensure privacy of health records—including those in federal agency databases—increasingly is at risk due to several trends. These include the growing use of information technologies in health care, structural changes in the health care delivery and payment systems, and information gathered from genetic testing. These factors accentuate the fact that existing legal safeguards to protect patient confidentiality are limited. In particular, concerns are raised about the increasing number of parties who have routine access to personally identifiable health records in institutions involved in health care treatment, payment, and oversight. The growth in the application of information technologies in all aspects of health care delivery also creates new vulnerabilities for patient confidentiality.

The passage of the Health Insurance Portability Act of 1996 (HIPAA, P.L. 104-191) has placed deadline pressure on Congress to consider medical records privacy legislation. HIPAA requires the Secretary of HHS to make recommendations to Congress on ways to protect individually identifiable information and to establish penalties for wrongful disclosure for health care transactions. The Secretary presented those recommendations on September 11, 1997. Congress has until August 1999 to enact a privacy law or else the Act requires HHS to promulgate regulations on privacy protection within the following 6 months.

The concept of a "code of fair information practices," which was recommended in early studies on privacy and is embedded in the Privacy Act of 1974, remains fundamental to all proposals today for maintaining confidentiality of personal records. Fair information practices include, among others, establishing conditions for disclosure of personally identifiable information, providing individuals with access to records held and the right to make corrections, and enforcing penalties for noncompliance.

While consensus exists on the need to implement fair information practices for health records, a number of unresolved issues remain. For example, there was much criticism of the HHS recommendations for allowing law enforcement officials to gain access to personally identifiable health records without additional safeguards beyond existing law. Finding the appropriate balance between access to health records for research purposes and individual privacy rights continues to be the subject of much debate. Whether state law should be preempted by a uniform national law is highly contentious. Reliance on patient consent as the primary mechanism for protecting privacy versus establishing legal and regulatory mechanisms that provide baseline protections also is a key question.

Over a dozen bills have been introduced in the 105th Congress to provide protection for medical records confidentiality and to ensure that individuals are not discriminated against based on genetic information. In addition, medical records confidentiality provisions are included in much broader legislation intended to regulate

---

[7] Prepared by Irene Stith-Coleman, Specialist in Biomedical Policy, Science, Technology, and Medicine Division.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 14 2002

health insurance through managed care plans (H.R. 4250 and S. 2330. H.R. 4250 passed the House on July 24, 1998 and has been placed on the calendar in the Senate).

Even as policymakers consider this legislation, several key issues remain. They include the following.

- **Federal preemption of state laws.** The question is the desirability of enacting federal medical privacy legislation that preempts, either in whole or in part, state privacy laws. In some areas of law, certain states are generally regarded as either having stronger privacy protections for certain types of information or as having acted in an area in the absence of federal law. Examples include the areas of mental health, public health reporting, and privileges (such as the physician-patient privilege).

- **Patient Identifiers.** The provisions of the Health Insurance Portability and Accountability Act direct the Secretary of HHS to promulgate standards for identifiers for certain purposes. Advantages might include administrative simplification, potentially reduced costs for institutions and reimbursement systems, and facilitating the linkage of valuable health data about a patient that might be useful in providing improved care. At the same time, personal identifiers raise serious privacy concerns, perhaps linking federal government medical data with financial data or employment information.

- **Patient Rights to Access.** A fundamental element of a code of fair information practices is the right of individuals to know about information being maintained about them and the right to amend incorrect records or supplement information. There appears to be strong consensus that these principles should be part of any legislation proposed to provide protection of medical records privacy.

- **Health Research.** Efforts to restrict the access of researchers to information in medical records may conflict with the goal of improving patient care. For example, observational outcome studies rely on existing medical records data. Many research projects, including those at federal research facilities, require the use of identifiable records, sometimes without the explicit consent of the individual. Researchers are concerned that legislative proposals seeking to provide strong privacy protections may result in serious limitations on the conduct of health studies that may offer important benefits to society.

See also:

Irene Stith-Coleman, *Medical Records Confidentiality.* CRS Issue Brief 98002. Updated regularly.

Irene Stith-Coleman and Angela Choy, *Genetic Discrimination Legislation in the 105th Congress: A Bill Comparison.* CRS Report 97-873. 31 December 1997.

Nancy Lee Jones, *Genetic Information: Discrimination and Privacy Issues.* CRS Report 96-808. 1 January 1998.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 15 2002

Domain Names [8]

During the 105th Congress, controversy surfaced over the disposition of the Internet domain name system (DNS). Internet domain names were created to provide users with a simple location name for computers on the Internet, rather than using the more complex, unique Internet Protocol (IP) number that designates their specific location. As the Internet has grown, the method for allocating and designating domain names has become increasingly controversial.

The Internet originated with research funding provided by the Department of Defense Advanced Research Projects Agency (DARPA) to establish a military network. As its use expanded, a civilian segment evolved with support from the National Science Foundation (NSF) and other science agencies. While there are no formal statutory authorities or international agreements governing the management and operation of the Internet and the DNS, several entities play key roles in the DNS. The Internet Assigned Numbers Authority (IANA) makes technical decisions concerning root servers, determines qualifications for applicants to manage country code Top Level Domains (TLDs), assigns unique protocol parameters, and manages the IP address space, including delegating blocks of addresses to registries around the world to assign to users in their geographic area. IANA operates out of the University of Southern California's Information Sciences Institute and has been funded primarily by the Department of Defense.

Prior to 1993, the National Science Foundation (NSF) was responsible for registration of nonmilitary generic Top Level Domains (gTLDs) such as .com, .org, .net, and .edu. In 1993, the NSF entered into a 5-year cooperative agreement with Network Solutions, Inc. (NSI) to operate Internet domain name registration services. In 1995, the agreement was modified to allow NSI to charge registrants a $50 fee per year for the first two years, of which 70% went to NSI to cover its costs and 30% was deposited in the "Intellectual Infrastructure Fund" to be reinvested in the Internet. Since the imposition of fees in 1995, criticism arose over NSI's sole control over registration of the gTLDs. In addition, there was an increase in trademark disputes arising out of the enormous growth of registrations in the .com domain. With the cooperative agreement between NSI and NSF due to expire in 1998, the Administration, through the Department of Commerce (DOC), began exploring ways to transfer administration of the DNS to the private sector.

In the wake of much discussion among Internet stakeholders, and after extensive public comment on a previous proposal, the DOC, on June 5, 1998 issued a final statement of policy, *Management of Internet Names and Addresses* (also known as the "White Paper"). The White Paper states that the U.S. government is prepared to recognize and enter into agreement with "a new not-for-profit corporation formed by private sector Internet stakeholders to administer policy for the Internet name and address system." In deciding upon an entity with which to enter such an agreement, the U.S. government will assess whether the new system ensures stability,

---

[8] Prepared by Lennard G. Kruger, Specialist in Science and Technology, Science, Technology, and Medicine Division.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 16 2002

competition, private and bottom-up coordination, and fair representation of the Internet community as a whole.

In effect, the White Paper endorsed a process whereby the divergent interests of the Internet community would come together and decide how Internet names and addresses will be managed and administered. Accordingly, Internet constituencies from around the world (calling themselves "the International Forum on the White Paper"or IFWP) held a series of meetings during the summer of 1998 to discuss how the New Corporation (NewCo) might be constituted and structured. In September of 1998, IANA, in collaboration with NSI, released a proposed set of bylaws and articles of incorporation for a new entity called the Internet Corporation for Assigned Names and Numbers (ICANN). The proposal was criticized by some Internet stakeholders, who claimed that ICANN does not adequately represent a consensus of the entire Internet community. Accordingly, other competing proposals for a NewCo were submitted to DOC. On October 20, 1998, the DOC tentatively approved the ICANN proposal. Pending the satisfactory resolution of several remaining concerns raised by the competing proposals -- including accountability, transparent decision-making processes, and conflict of interest -- the DOC will begin work on a transition agreement with ICANN. On November 6, ICANN announced that it had submitted a revised set of corporate bylaws to DOC which are intended to address DOC concerns. Meanwhile, nine members of ICANN's interim board have been chosen (four Americans, three Europeans, one from Japan, and one from Australia).

The White Paper also signaled DOC's intention to ramp down the government's Cooperative Agreement with NSI, with the objective of introducing competition into the domain name space while maintaining stability and ensuring an orderly transition. On October 6, 1998, DOC and NSI announced an extension of the Cooperative Agreement between the federal government and NSI through September 30, 2000. During this transition period, government obligations will be terminated as DNS responsibilities are transferred to the NewCo. Specifically, NSI has committed to a timetable for development of a Shared Registration System that will permit multiple registrars (including NSI) to provide registration services within the .com, .net., and .org gTLDs. By March 31, 1999, NSI will establish a test bed supporting actual registrations by five registrars who will be accredited by the NewCo. According to the agreement, the Shared Registration System will be deployed by June 1, 1999, and fully implemented and available to all accredited registrars by October 1, 1999. NSI will also continue to administer the root server system until receiving further instruction from the government.

During the 105th Congress, a number of DNS hearings were held by the House Committees on Science, on Commerce, and on the Judiciary. The hearings explored issues such as governance, trademark issues, how to foster competition in domain name registration services, and how the Administration will manage and oversee the transition to private sector ownership of the DNS. Most recently, the House Committees on Commerce and on Science held hearings on June 10 and October 7, 1998, respectively. On October 15, the Chairman of the House Committee on Commerce sent letters of inquiry to DOC and the White House reflecting concerns that the process which produced the ICANN proposal was insufficiently open and responsive to the interests of all Internet stakeholders.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 17 2002

One of the thorniest issues surrounding the DNS is the resolution of trademark disputes that arise in designating domain names. In the early years of the Internet, when the primary users were academic institutions and government agencies, little concern existed over trademarks and domain names. As the Internet grew, however, the fastest growing number of requests for domain names were in the .com domain because of the explosion of businesses offering products and services on the Internet. Since domain names have been available from NSI on a first-come, first-serve basis, some companies discovered that their name had already been registered. The situation was aggravated by some people registering domain names in the hope that they might be able to sell them to companies that place a high value on them and certain companies registering the names of all their product lines.

The increase in conflicts over property rights to certain trademarked names has resulted in several lawsuits. Under the current policy, NSI does not determine the legality of registrations, but when trademark ownership is demonstrated, has placed the use of a name on hold until the parties involved resolve the domain name dispute. The White Paper calls upon the World Intellectual Property Organization (WIPO) to convene an international process, including individuals from the private sector and government, to develop a set of recommendations for trademark/domain name dispute resolutions. WIPO is developing recommendations and is scheduled to present them to the NewCo in March 1999. Meanwhile, the Next Generation Internet Research Act of 1998 (P.L. 105-305) directs the National Academy of Sciences to conduct a study of the short and long-term effects on trademark rights of adding new generic top-level domains and related dispute resolution procedures.

Another DNS issue relates to the disposition of the Intellectual Infrastructure Fund, derived from domain name registration fees collected by NSI. The fund grew to $56 million before NSF and NSI discontinued collecting fees for the fund as of April 1, 1998. A number of suggestions were offered for use of the fund, including returning money to registrants, setting up a nonprofit entity to allocate funds, or using it for global administrative projects, such as Internet registries in developing countries. The VA/HUD/Independent Agencies FY1998 Appropriations Act (P.L. 105-65) directed NSF to credit up to $23 million of the funds to NSF's Research and Related Activities account for Next Generation Internet activities. A class action suit filed by six Internet users against NSF and NSI in October 1997 questioned the legal authority of NSF to allow NSI to charge for registering Internet addresses and requested $55 million in refunds. The suit also sought to prevent the government from spending the money as directed by Congress. On April 6, 1998, U.S. District Judge Thomas Hogan dismissed the charge that NSF lacked authority to permit NSI to collect fees, but let stand another charge challenging the portion of the fee collected for the infrastructure fund. However, the FY1998 Emergency Supplemental Appropriations Act (P.L. 105-174), enacted on May 1, 1998, contains language ratifying and legalizing the infrastructure fund. Accordingly, Judge Hogan reversed his decision, thereby allowing NSF to spend the $23 million from the fund through FY1999 on the Next Generation Internet program.

See Also:

Jane Bortnick Griffith and Lennard G. Kruger, *Internet Domain Names: Background and Policy Issues,* CRS Report 97-868. 7 December 1998.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 18 2002

Electronic Commerce [9]

On July 1, 1997, the Clinton Administration released its report, *A Framework for Global Electronic Commerce*. This report provided several policy recommendations for enhancing electronic commerce on the Internet, and outlined where the U.S. private sector should continue to develop electronic commerce, and those areas where federal government policies are appropriate for oversight and regulation of electronic commerce. The report provided four overarching principles to guide federal policy, and nine specific policy areas where the principles would be applied. Congress has responded to many of these principles and policy areas, including taxation of electronic commerce.

The Clinton Administration's interest in global electronic networks was addressed in President Clinton's first term. In 1994, Vice President Gore gave a speech in Buenos Aires, Argentina calling for the establishment of a global network of networks—what he described as a Global Information Infrastructure (GII). The GII would be the international counterpart to the Administration's National Information Infrastructure (NII). The NII was introduced in 1993 as a policy platform in which the Clinton Administration would use public and private sector partnerships to strengthen and expand the nation's information networks. Vice President Gore drew upon the NII when proposing the GII, expanding national policy to global policy. The Vice President stated that three major developments could arise from the creation of a GII: its applications could result in greater democracy worldwide, it could act as a catalyst for economic growth and more global trade among all nations, and it could become an important element for sustainable growth for lesser developed and developing nations.

The Administration repeated these principles at a G-7 meeting in Brussels, Belgium in February 1995. The topic of this G-7 meeting was to address what international policies could result in greater liberalization of global telecommunications policies and connections. While the representatives of many nations supported the U.S. GII position, others raised concerns about the reciprocity of global commerce without multilateral agreements to ensure compliance by all nations.

Subsequent international telecommunications conferences and agreements brought more discussion on the best way to further open global electronic commerce. On February 5, 1998 an agreement reached by 70 countries under the auspices of the World Trade Organization (WTO) went into effect. The WTO telecommunications services agreement is expected to liberalize trade in basic telecommunications services, benefit U.S. telecommunications companies by permitting them greater entry into foreign markets, and facilitate economic growth. This agreement came almost two years to the day after the Telecommunications Act of 1996 (P.L. 104-104) was signed into law by President Clinton, significantly deregulating much of the U.S. telecommunications market and opening it to greater competition.

---

[9]Prepared by Glenn J. McLoughlin, Specialist in Technology and Telecommunications Policy, Science, Technology, and Medicine Division.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 19 2002

Still, some concerns remain regarding security and privacy, taxation, and export control policy in global networks. Many contend that since the Internet already is a global, cooperative network of networks with a multitude of users, there is little need for government (or governments) to further regulate or oversee commercial development. Others, however, contend that as electronic commerce expands, a new framework will be needed to help ensure the integrity and safety of transactions on global networks.

The July 1997 Administration report used the GII policy as the foundation for establishing four principles to guide U.S. policy on electronic commerce. They are:

- **The private sector should lead.** For electronic commerce to flourish, the Administration stated that the private sector should lead in the continued innovation, services, participation, and pricing of electronic commerce on the Internet.

- **Governments should avoid undue restrictions on electronic commerce.** Parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet, with minimal government involvement or interference.

- **Government involvement, if needed, should be predictable, minimalist, and consistent.** There may be instances where regulation of the private sector may be needed, or national interests supersede commerce. However, the Administration contends that government policies should establish a predictable and simple legal environment, not top-down administrative regulation.

- **The Internet is unique—and this quality should be maintained.** Governments should recognize the unique qualities of the Internet, which includes its decentralized nature and its open access. Regulatory frameworks that may not fit these qualities should be reviewed and possibly revised, rather than constraining electronic commerce possibilities on the Internet.

In turn, the Clinton Administration advocated that these four principles should be applied to nine policy areas: taxation, payments, a uniform commercial code, intellectual property rights, privacy, security, infrastructure, content, and standards. Like the GII and G-7 discussion in Brussels, these principles and policy areas are intended to be global in scope and application. The Administration cautions against a handful of nations making electronic commerce policy decisions without a broad consensus from the rest of the world.

In the 105th Congress, some of these issues, such as privacy and security, were already being addressed within the context of the existing debate of U.S. policies for medical records and encryption, which also had significant global ramifications. In other areas, such as standards and intellectual property protection, the Congress has examined the use of multinational organizations, like the World Trade Organization, to both address these issues and to seek reforms.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 20 2002

One area, however, which did not fit cleanly into an existing domestic or international policy issue was the issue of taxation of electronic commerce on the Internet. During the 105th Congress, this has become a very contentious issue. The Clinton Administration's report recommends that there be no new taxation of electronic commerce on the Internet by federal, state, or local governments. The Administration has contended that economic growth from electronic commerce would offset any losses of federal revenue, and that ultimately successful electronic commerce will mean higher corporate profits, which are taxed. Generally, the U.S. industry has supported this position. However, many U.S. state Governors have contended that sales tax revenue from electronic commerce could be an important part of states' revenue base, and have opposed the Administration's position.

The 105th Congress considered six bills that would either temporarily or permanently suspend taxation of Internet access and electronic commerce. One bill, The Internet Tax Freedom Act (H.R. 4105), was passed by both houses of Congress and was included as part of the FY1999 Omnibus Appropriations Act (P.L. 105-277). This law creates a three year moratorium on the ability of state and local governments to tax electronic commerce. During this time, an advisory commission on electronic commerce would examine this issue and report within two years back to the Congress and the President on its findings of tax policy and electronic commerce. It is likely that the 106th Congress will monitor this issue and conduct additional oversight hearings in the coming year.

See also:

Nonna A. Noto, *Internet Tax Bills in the 105th Congress.* CRS Report 98-509. 21 August 1998.

Nonna A. Noto, *Internet Tax Freedom Act: H.R. 4105 as Passed by the House.* CRS Report 98-597. 9 July 1998.

Bernard A. Gelb, *Telecom Services: The WTO Agreement.* CRS Report 98-165. 26 February 1998.

Angele A. Gilroy, *The Telecommunications Act of 1996 (P.L. 104-104).* CRS Report 96-223. 2 July 1997.

The Internet and the Federal Role [10]

The Internet is an international, cooperative computer "network of networks" that links many types of users, such as governments, schools, libraries, corporations, hospitals, individuals, and others. No single organization owns, manages, or controls the Internet. However, the Internet is not free. The major costs of running the network are shared by its primary users: universities, national laboratories, high-tech corporations, and governments.

---

[10]Prepared by Rita Tehan, Information Research Specialist, Congressional Reference Division and Glenn J. McLoughlin, Specialist in Technology and Telecommunications Policy, Science, Technology, and Medicine Division.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 21 2002

The original network, ARPANET, was created in the late 1960s. Its purpose was to allow defense contractors, universities, and Department of Defense staff working on defense projects to communicate electronically and to share the computing resources of the few powerful, but geographically separate, computers of the time. By 1983, the term "the Internet" came into use to describe the concept of interconnecting networks.

In 1985, the National Science Foundation (NSF) funded several national supercomputer centers, with the intention of making these supercomputer centers available to the research community in universities across the country. Many state and regional universities had already developed local and regional networks. The NSF funded a network linking the five original supercomputer centers, and offered to let any of the regional and university computer centers that could physically reach this network connect to it. This was the "seed" of the Internet network as we know it today, and the original reason to connect to it was for remote access to supercomputer facilities.

In November 1987, NSF awarded a contract to several private sector firms and the state of Michigan to upgrade and operate the NSF Network (NSFnet) backbone. The purpose of the NSFnet backbone by this time was to link the growing "regional" networks set up by various university systems. In 1990, ARPANET ceased operation because NSFnet and various midlevel networks sponsored by NSF made the Internet viable for commercial traffic. DOD continues to run a military network. A number of universities linked to the NSFnet to gain access to the supercomputers. But besides research, they found that the network was useful for electronic mail, file transfer, and news groups. The traffic on the network rose fairly dramatically.

In May 1993, NSF radically altered the architecture of the Internet, because the government wanted to get out of the backbone business. In its place, NSF designated a series of Network Access Points (NAPs), where private commercial backbone operators could "interconnect." In 1994, NSF announced that four NAPs would be built, in San Francisco, New York, Chicago, and Washington, DC.

On April 30, 1995, the NSFnet backbone was essentially shut down, and the NAP architecture became the Internet. The Internet backbone, the first level of connection to the Internet, now known as very-high-speed backbone network services (vBNS), is maintained by IBM Corp., MCI Communications, and Merit (a nonprofit organization owned by 11 public universities in Michigan). Internet access is also provided via Internet Service Providers such as America Online, MCI, Sprint, MindSpring, AT&T, Netcom, EarthLink, Concentric, SpryNet, and Microsoft Network.

In October 1996, President Clinton proposed the Next Generation Internet (NGI) initiative. This is a plan to build a national network that connects universities and federal research organizations at rates 100 to 1,000 times faster than today's Internet. Seed money for development of the network will go to DOD, the Department of Energy, the National Aeronautics and Space Administration, and NSF.

The first goal of the NGI initiative is to research, develop, and experiment with advanced network technologies that will provide dependability, diversity, security, and

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 22 2002

real-time capability for applications. The second goal of the NGI initiative is the development of the next generation network testbed. This effort will overcome today's "speed bumps" that slow end-to-end usable connectivity; the slowing is caused by incompatibilities in performance capabilities.

Federal agencies supporting the NGI are now creating a high performance distributed laboratory consisting of 100 sites at universities, federal research institutions, and other research partners. The first goal is to achieve computing speeds in excess of 100 times that of today's Internet. It will serve as a testbed for hardware, software, protocols, security, and network management. Second, the federal NGI effort will develop ultrahigh-speed switching and transmission technologies and end-to-end network connectivity at more than 1 gigabit per second. Such networks will be high-risk, pioneering networks limited to 10 NGI sites at speeds 1,000 times faster than today's Internet.

Many agencies and research universities are already working on related communications projects, including the less ambitious Internet2 (I2) project. The I2 was started in 1996 by 30 universities and piggybacks on a network that the NSF uses to connect the country's federal supercomputer centers. The I2 network's top speed currently is about 100 times the speed of the public Internet. The I2 project is slated to provide high-capacity communications links among the 100 top research universities that run the project. Many of these universities receive extensive government grants for technology research. Clinton Administration officials contend that it is likely that every major city in the United States will have its own I2 connection, or gateway, within the next 5 years.

The Internet offers almost limitless possibilities for the free communication of ideas, research, and information. However, the Internet is not free. Some of the networks are partially funded by certain government agencies, especially the NSF and other science agencies, for use by scientists, researchers, and the education community. Still, the major costs of running the network are shared by its primary users: universities, national laboratories, high-tech corporations, and governments. Each institution, organization, corporation, or individual with access to the Internet purchases that access.

The Internet also depends on cooperation and it is difficult to guarantee consumer privacy, document authenticity, or protection from unwanted advertising, messages, or information. The National Infrastructure Protection Center (NIPC), whose mandate is to detect, prevent and respond to cyber and physical attacks on U.S. computer systems, will have links to other government departments such as Defense, State, and Treasury, as well as to local and international police agencies. (See the section: "Information Infrastructure and National Security").

One area of concern is how accessible the Internet will be to the poor and less educated. Many people cannot afford a computer and modem, and in remote areas some users pay long-distance telephone charges to gain access to the Internet. Individuals who do not have access through libraries, school, or work may miss opportunities to retrieve useful information and to participate in an electronic community. Many policymakers are pursuing proposals to ensure widespread access to networked information through schools, libraries, and other public service

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 23 2002

institutions. Citizens' access to information in federal agencies and other government repositories is an important component of this issue of information technology "haves" and "have nots."

See also:

Rita Tehan, *The Internet: History, Infrastructure, and Selected Issues.* CRS Report 98-649. July 28, 1998

Marcia S. Smith, Jane Bortnick Griffith, Richard M. Nunno, and John D. Moteff. *Internet: An Overview of Six Policy Issues Affecting Its Use and Growth,* CRS Report 98-67. 21 August 1998.

Glenn J. McLoughlin, *The National Information Infrastructure: The Federal Role.* CRS Issue Brief 95051. Updated regularly.

Glenn J. McLoughlin, *Next Generation Internet.* CRS Report 97-521. 8 June 1998.

Angele A. Gilroy, *Telecommunications Discounts for Schools and Libraries: The "E-Rate" Program and Controversies.* CRS Issue Brief 98040. Updated regularly.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 24 2002

Document No. 173

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [i] 2002

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [ii] 2002