The United States Senate
Special Committee on the Year 2000 Technology Problem

Senator Robert F. Bennett, Chairman
Senator Christopher J. Dodd, Vice-Chairman

Y2K Aftermath – Crisis Averted
Final Committee Report

Summary of Committee Findings

FEBRUARY 29, 2000

MEMBERS

Robert F. Bennett, UT, Chairman
Christopher J. Dodd, CT, Vice-Chairman

Jon Kyl, AZ
Gordon Smith, OR
Richard G. Lugar, IN
Ted Stevens, AK, *Ex Officio*

Daniel Patrick Moynihan, NY
John Edwards, NC
Robert C. Byrd, WV, *Ex Officio*

STAFF

Robert Cresanti , Staff Director
T.M. (Wilke) Green, Minority Staff Director
John B. Stephenson, Deputy Staff Director
Thomas J. Bello, Professional Staff
Tania L. Calhoun, Committee Counsel
James P. Dailey, Professional Staff
Paul Hunter, Professional Staff
Unice Lieberman, Minority Press Secretary
Sara Jane MacKay, Legislative Correspondent
Don Meyer, Press Secretary
J. Paul Nicholas, Professional Staff
Frank Reilly, Professional Staff
Noelle Busk Ringel, Archivist
Amber Sechrist, Clerk
Ronald L. Spear, Professional Staff
Deborah Steward, GPO Representative

S. Prt. 106-XX

The United States Senate
Special Committee on the Year 2000 Technology Problem

Senator Robert F. Bennett, Chairman
Senator Christopher J. Dodd, Vice-Chairman

Y2K Aftermath – Crisis Averted
Final Committee Report

SUMMARY OF COMMITTEE FINDING
FEBRUARY 29, 2000

February 29, 2000

Dear Colleague:

Having fulfilled its oversight and fact-finding mission following the world's successful navigation of the millennium date change, the U.S. Senate Special Committee on the Year 2000 Technology Problem will disband on February 29, 2000, in accordance with its charter.

Today, we issue the Committee's final report. This report provides the best information available on the occurrence of Y2K glitches in the United States and abroad. While problems will continue to appear throughout the year, most documented domestic Y2K-related events have thus far been minor, localized, and short-lived. Internationally, there have been fewer problems than predicted.

The report also discusses lessons learned and benefits derived from Y2K. Minor consequences aside, Y2K has spurred the modernization of our nation's technology base and positioned it for continued economic growth. In addition, the Y2K readiness experience has taught us valuable lessons about the nation's technological dependencies, interconnections, and vulnerabilities. These lessons will prove invaluable as Congress examines new policies addressing critical infrastructure protection and future information technology issues.

Robert F. Bennett
Chairman

Christopher J. Dodd
Vice Chairman

{NOTE: FORMAL RELEASE INCLUDES THE SIGNATURES OF ALL COMMITTEE MEMBERS}

TABLE of CONTENTS

APPENDICES

This page left intentionally blank. (p.2)

OVERVIEW

Since its April 1998 inception, the U.S. Senate Special Committee on the Year 2000 Technology (Y2K) Problem has pursued the following goals: (1) to study the Y2K problem's potential impact on all levels of government and the private sector—both in the U.S. and abroad; (2) to make findings of fact and serve as a repository for accurate Y2K information; (3) to increase awareness about the Y2K problem; and (4) to make recommendations regarding new legislation and existing laws to incentivize Y2K preparation. Having fulfilled these objectives, the Committee will disband on February 29, 1999, in accordance with its charter.

The Committee's final report is comprised of three sections. The first describes how well the nation and the world transitioned to the Year 2000, including examples of reported computer problems. The second section describes lessons learned and benefits derived from Y2K. Finally, the third section examines how these benefits and lessons might be used to better address future information technology (IT) challenges.

Hundreds of computer problems have been reported since January 1, 2000, but most have been quickly corrected and none have caused serious disruptions. While Appendix II of this report includes examples of computer problems that have occurred since the date change, the full extent of Y2K problems will probably never be known. There is no incentive for corporations or countries to publicly report problems. Instead, they will simply fix these problems and continue their operations.

The U.S. spent an estimated $100 billion ($8.5 billion within the federal government alone) on the Y2K problem, and the positive results domestically were not unexpected. Several factors contributed to a relatively uneventful Y2K rollover. In addition to the unprecedented level of effort undertaken by most organizations, the sharing of information, focus on supplier interrelationships, and attention to contingency planning all contributed to a smooth transition. Committee hearings and work in late 1999 also revealed a significantly lower failure rate than predicted for embedded chips.

It is the Committee's judgment that the level of effort was justified and the expenditure of funds was indeed necessary. Testimony and available research during 1998 and early 1999 convinced the Committee that the Y2K threat was very real, and that the risks and consequences of inaction were too dire to justify a lesser effort. Even considering the enormous amount of time and money spent on Y2K, the level of success is still remarkable considering that the U.S.—with one-fourth of the world's computer assets—is the most technologically dependent nation on earth.

While the positive results of domestic Y2K preparation were not unexpected, the low level of disruption internationally was somewhat surprising. Several factors may have contributed to inaccurate predictions and better-than-expected results abroad. Among these were (1) the difficulty in obtaining accurate and current information about the technology dependencies and Y2K preparedness levels of other countries; (2) the underestimation of the amount of remediation that actually occurred in the last two months of 1999; (3) the underestimation of the economic influence of multinational corporations on the preparedness of their host countries; and (4) the fact that contingency plans for countries behind in Y2K remediation worked better than expected.

In addition, in many cases, infrastructure entities and companies switched to manual operations and/or had additional personnel on standby during the rollover. This action allowed problems to be quickly addressed and, as a result, prevented more failures from occurring.

Not all Y2K problems, however, were expected to occur and be resolved in the first few weeks or months following January 1, 2000. In addition to vulnerabilities surrounding February 29, several problems may yet occur as quarterly and annual business cycles continue. The Committee expects continued reports of minor nuisances throughout 2000, but no major problems.

Also during 2000 and beyond, government and private sector organizations must undertake permanent software fixes where temporary patches were utilized. Organizations may need to address non-mission critical systems where repairs were postponed. Internationally, most fixes were temporary clock rollbacks that must be fixed permanently at some point.

In addition to avoiding major Y2K problems, enduring lessons have been learned and benefits derived from the remediation experience. Most significantly, the IT infrastructure and mechanisms for more effectively managing it have been modernized. Also, Y2K has caused a heightened level of knowledge among executive-level managers as to the importance and vulnerabilities of information technology. Critical infrastructure protection and other IT issues now rank higher among the mission priorities of corporate and government executives. Finally, new public/private partnerships and more effective avenues of communication—domestically and internationally—have been created that will be beneficial in addressing future IT challenges.

The Committee believes that improving critical infrastructure protection will be the next major challenge to the IT community. Hacking, cyber theft/terrorism and information warfare have the potential to negatively impact e-commerce and impede overall economic growth.

Funding for national infrastructure protection is currently spread over 15 agencies overseen by nine congressional committees. This presents numerous challenges to effective congressional oversight and policy initiatives. The Senate must examine the congressional structure and its efficacy for addressing critical infrastructure protection and future IT issues.

* * * *

Many thousands of people deserve credit for the Y2K success story. A few deserve special recognition.

In 1996, Senator Daniel Patrick Moynihan commissioned a Congressional Research Study of Y2K's potential impact. He also contacted President Clinton to urge the appointment of a presidential aide to direct federal Y2K efforts.

> ***"There are many individuals who deserve a great deal of credit for the Y2K success story—Pat Moynihan, Alan Greenspan, John Koskinen, Arthur Levitt, and Stephen Horn—just to name a few"***
>
> ***-- Senator Bennett***

Federal Reserve Chairman Alan Greenspan offered valuable assessments with regard to Y2K and its potential impact on investors and the U.S. economy. His assessments warded off potentially destructive Y2K-related behavior such as inventory stockpiling and divestment in U.S. markets. He also drew attention to the high level of preparedness in private industry and in U.S. markets, helping to avoid a Y2K-induced economic downturn.

The President's Council on Year 2000 Conversion, chaired by Special Assistant to the President John Koskinen, performed a valuable service to the nation by working to guarantee the functioning of vital public services. Mr. Koskinen effectively formed coalitions between the public and private sectors, and initiated and monitored Y2K preparation among federal, state, and local governments, as well as different infrastructure sectors and industries. He also kept Congress and the public informed with regard to progress.

SEC Chairman Arthur Levitt was influential in fostering cooperation among private industry and the financial services sector. In response to Senator Bennett's introduction of S.1518, the SEC clarified federal securities disclosure law to remind municipal securities issuers, public companies, investment advisers, and investment companies that anti-fraud provisions included Y2K disclosure. The SEC also took action against broker-dealers who failed to report Year 2000 readiness, and issued a report on the Y2K preparedness of publicly traded companies.

Congressman Stephen Horn, Chairman of the Government Reform Subcommittee on Government Management, Information and Technology, led oversight efforts in the U.S. House of Representatives regarding federal government preparedness. Through numerous hearings and quarterly report cards on federal preparedness, Congressman Horn exercised effective oversight of federal agencies.

THE RESULTS OF Y2K

This section assesses the effectiveness of the Y2K Information Coordination Center (ICC) and other “Day One” activities. It also includes a summary of Y2K problems comprised of the best information available in the U.S. and abroad. While problems will continue to appear throughout the year, documented Y2K-related events in the U.S. have so far been minor, localized, and short-lived. Internationally, there have been fewer problems than predicted.

DAY ONE PREPARATION/ PERFORMANCE

“Day One Preparation” refers to the operational plans devised at all levels of government and many private organizations to manage the January 1, 2000 date-change transition. Day One Preparation efforts represented the largest simultaneous mobilization of resources in anticipation of a potential disaster or emergency. Governmental Day One Preparation included the ICC’s establishment of a broad communications and reporting network, and the staffing of emergency operations centers by the Federal Emergency Management Administration (FEMA) and emergency management agencies at municipal, county, and state levels.

In private industry, Day One Preparation typically involved increased staffing of business and industry locations to both monitor and test key systems as the date roll-over occurred, and to provide immediate on-premise technical assistance in the event of failures. In many cases, trade associations established command centers to gather information about the status of critical infrastructures within a specific industry.

The ICC’s structure linked the Day One Preparation activities of the federal government and those of private industry. In essence, the same mechanism established by the President’s Council to track progress on Y2K preparedness throughout 1998 and 1999 served as the backbone of a Day One Preparation plan that was international in scope. Industry sector working groups already established by the President’s Council provided the foundation for large-scale Day One Preparation plans for the ICC. (The structure and organization of the President’s Council and the ICC were discussed in detail in the Committee’s first two reports.)

Several days prior to and after the date transition, Committee staff manned an operational desk at the ICC and utilized the Information Collection and Reporting System (ICRS), the ICC’s primary data collection system. The ICRS allowed the user to review the status of each sector, including government services, finance, transportation, power and water utilities, telecommunications, health care, and business. An “exception-based” three-tiered reporting system was used whereby contributors reported incidents having a potential impact on the presumed "green" or normal operating status of their sectors.

Incidents bearing any significant impact on any sector would have resulted in a change of rating from "green" to "yellow" (cautionary) or "red" (indicating significant disruption). John Koskinen, Chair of the President's Council, provided regular press briefings on reported incidents from the ICC throughout the week prior to and following the date-change transition. Transcripts of these briefings are available on the President's Council's/ICC web page at www.y2k.gov.

ICC staffing consisted of a central administrative staff, representatives of the various executive branch agencies, and contractors who provided data systems support. The President's Council estimated that approximately 175 to 200 people staffed the ICC.

Despite the late start in organizing the ICC, and despite problems experienced during the December 1999 ICRS system exercise phase, the ICC appears to have successfully accomplished its mission related to Day One Preparation. Several strong points in the ICC's operations are worthy of note. Although it was expressly not intended to serve as a decision-making body, on-site staffing of the ICC included many high-ranking officials from the various federal agencies. This would have been of great benefit had any major crisis developed as a result of the date-change transition. The immediate on-site presence of "command-level" officials could have served to streamline communications efforts if a national crisis had occurred. The ICC's effective degree of coordination among decision-makers from a broad variety of both public and private agencies was a significant accomplishment. Unlike law enforcement, military, and intelligence agencies, other entities providing information to the ICC were not operationally oriented and did not typically provide "real time" incident reporting. While the need to establish a reporting network that could feed information into the ICC presented a unique challenge to some agencies, this function was effectively performed.

Y2K was the first instance during which emergency managers in all 50 states and the U.S. territories were simultaneously operational and in direct communication with FEMA in anticipation of a single-source disaster or hazard.

FEMA's Y2K preparedness activities had a broad impact on Day One Preparation efforts at all levels of government, and on individual preparedness. FEMA used approximately 800 employees during the rollover, with personnel assigned to its Emergency Support Team at headquarters, the Mount Weather Emergency Assistance Center, FEMA's ten regional operational offices, its regional operations centers, state liaisons, and the ICC.

Many benefits were realized as a result of Day One Preparedness activities in the emergency management community:

- Existing emergency management systems were tested and stressed in response to a unique hazard;
- Increased attention was given to emergency preparedness at the individual and organizational levels;
- Disaster plans were revised and updated in many local communities and states;
- Relationships between various Federal Response Plan (FRP) agencies were strengthened;
- The value of the FRP to a broad range of potential disasters was reinforced;
- The application of the ICC's infrastructure failure reporting system is being evaluated by FEMA and the individual states; and
- Emergency services improved their abilities to function if affected by major emergencies or disasters.

The importance of Day One Preparedness was reinforced in the months approaching the date transition as law enforcement and intelligence concerns grew about the potential for Y2K/millennium-focused violence by domestic extremists and foreign terrorists. Had any large-scale events occurred, the communications networks initiated by organizations as part of Y2K Day One Preparations, and the pre-activation of emergency operations centers across the nation, would have dramatically increased the nation's ability to respond.

SUMMARY OF Y2K PROBLEMS

While hundreds of computer problems have been reported since January 1, 2000, most have been quickly corrected and none have caused serious disruptions. Because there is no incentive for corporations or countries to openly report problems, the full extent of Y2K's impact may never be known. Indeed, it is interesting to note that official government reports from around the world report far fewer incidents than reported by news services. For example, 32 countries including Australia, Brazil, Great Britain, Canada, Germany, and Norway reported no incidents on the official International Y2K Cooperation Center's website despite the fact that many incidents were reported in these countries by reliable news services.

Examples of domestic problems have included Medicare payment delays, double-billing by some credit card companies, degradation of a spy satellite system, 911 problems in several localities, and a nuclear weapons plant system anomaly. International events included non-safety-related problems at a nuclear power plant, a Hong Kong Futures Exchange outage, and a variety of biomedical device glitches. Despite these incidents, no major problems were experienced in the U.S. or worldwide during the millennium date change. Additional examples of reported computer problems are included in Appendix II. While the Committee was unable to verify these reports first-hand, the Appendix includes only those reports from sources considered reliable.

The U.S. spent an estimated $100 billion ($8.5 billion within the federal government alone) on the Y2K problem, and the positive results domestically were not unexpected. Several factors contributed to a relatively uneventful Y2K rollover. In addition to the unprecedented level of effort undertaken by most public and private organizations, information sharing, a focus on supplier interrelationships, and attention to contingency planning all contributed to a smooth transition.

Committee hearings also revealed a significantly lower failure rate than predicted for embedded chips. Analysis of testing during the last quarter of 1999 predicted an embedded chip failure rate of .001%, rather than the 2-3% failure rate projected in late 1998 and early 1999.

In the Committee's judgment, the level of effort was justified, and the expenditures of the public and private sectors were indeed necessary. Testimony and available research during 1998 and early 1999 convinced the Committee that the Y2K threat was real, and that the risks and consequences of inaction were too dire to justify a lesser effort. Despite the expense, the success of domestic Y2K preparation is remarkable, considering that the U.S.—with one-fourth of the world's computer assets—is the most technologically dependent nation on earth.

While the positive results of domestic Y2K preparation were not unexpected, the low level of disruption internationally was somewhat surprising. The following factors may have contributed to inaccurate predictions.

First, despite the efforts of the United Nations, World Bank, the International Y2K Cooperation Center and others, it was difficult to obtain accurate and current information about the technological dependencies and Y2K preparedness of other countries. The Y2K experience revealed that little is known about the level of automation in other countries' infrastructures, such as electric power or telecommunications.

Second, the amount of remediation occurring in the last two months of 1999 may have been underestimated. Countries that delayed Y2K remediation greatly benefited from the lessons learned by countries leading the world in Y2K compliance, allowing laggard countries to make Y2K repairs more quickly and efficiently than previously thought possible. In addition, many countries and organizations simply rolled back computer clocks, which allows the temporary claim of compliance but fails to address long-term date dependency problems.

Third, the economic influence of multinational corporations was underestimated. Global corporations aggressively addressed the Y2K problem at international facilities, and had a profound influence on the preparedness of host countries and their attendant infrastructures.

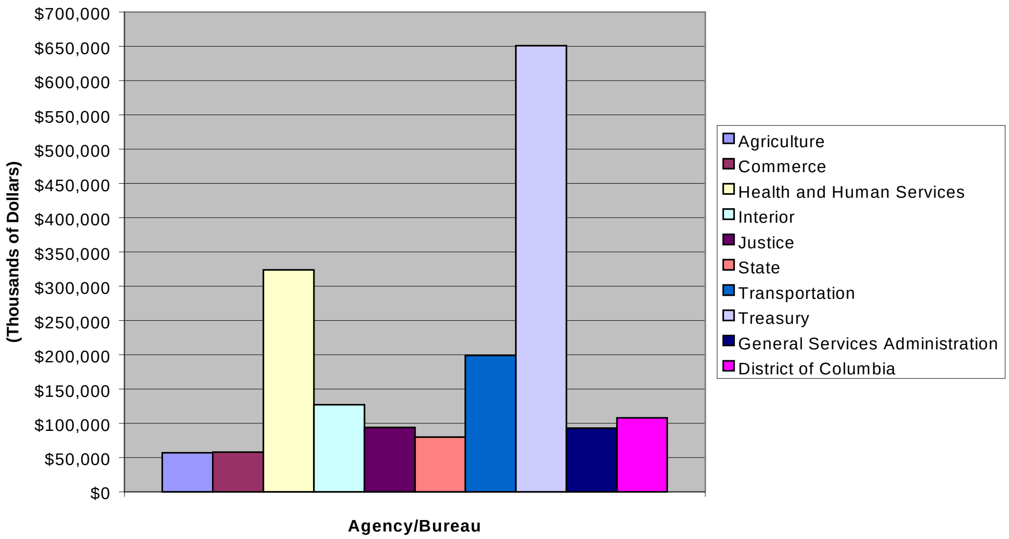
Fourth, many countries began addressing theY2K problem so late that contingency planning was their only option. In many cases, infrastructure entities and companies switched to manual operations and/or had additional personnel on standby during the rollover. This allowed problems to be quickly addressed and may have prevented more failures from occurring.

THE COSTS OF Y2K

Preparations to avoid and/or mitigate Y2K-related problems proved to be one of the most complex and vast management challenges in recent history. From roughly 1995-1999, private and public organizations, both domestically and internationally, mobilized huge resources to address Y2K. Although no universal cost-estimating processes were agreed upon, many organizations estimated cost of Y2K in terms of lines of code to be assessed, remediated, and tested. One dollar per line of code was one widely-used cost estimate, but the worldwide cost of preparing for Y2K may never be known.

However, the Office of Management and Budget estimated that federal government Y2K spending reached $8.34 billion; the Commerce Department estimated that U.S. government and businesses spent about $100 billion; and a journalist for Newsweek estimated global Y2K

Y2K Emergency Supplemental Funds



spending at $500 billion.[1]

Congress appropriated $3.35 billion in Y2K emergency supplemental funding: $1.1 billion for the DOD and $2.25 billion for non-defense departments and agencies. Of the non-defense emergency supplemental spending, the top 10 agencies/departments receiving funds are depicted in the chart above.

Most analysts agree that Y2K spending was higher per capita in the U.S. than in other industrialized countries such as Italy, Spain, and Russia.[2] Many argue, however, that the U.S. is far more computerized than those countries. U.S. systems are also more interconnected and complex than in most other countries, leading to a higher cost for Y2K remediation here at home.

Finally, countries that started Y2K remediation later than the U.S. had the benefit of U.S.-developed diagnostic software tools, experience, and access to public information about the compliance process.

IS THE CRISIS OVER? PROGNOSIS FOR THE MONTHS AHEAD

Not all Y2K problems were expected to occur and be resolved in the first few weeks or months following January 1, 2000. In addition to vulnerabilities surrounding February 29, several problems may yet occur as quarterly and annual business cycles continue. The Gartner Group estimated that peak Y2K problem periods would be in mid-2000, with some problems lingering into 2003. The Committee also expects continued reports of minor nuisances throughout 2000, but no major problems.

Pre- and post-Y2K analysis has included hypotheses regarding the potential for future Y2K problems. Future date-related problems have been predicted for computer systems that may not recognize 2000 as a leap year. Another potential problem has been predicted for 2038, when timers in some UNIX operating systems roll over much like the GPS systems clocks did in August 1999.

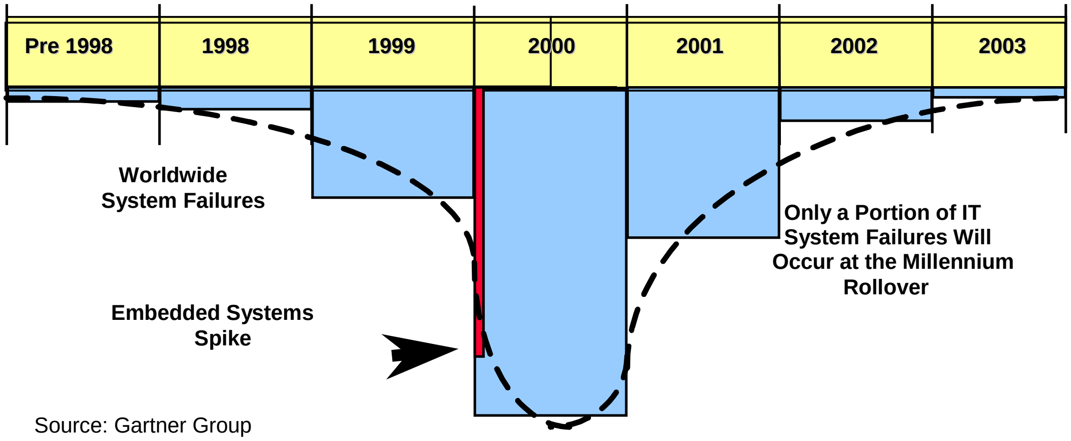
The Committee's investigation concludes that, given the evolution of the Y2K scenario since December 31, 1999, there will be few lingering and long-term effects from Y2K. Organizations working on the problem were generally well aware of potential glitches associated with the leap year, and were actively preparing for February 29, 2000. The U.S. Navy, for example, demonstrated to Committee staff a successful rollover drill during naval battle group operations in 1999.

[1] In addition, the Gartner Group estimated that the U.S. spent $150-$225 billion. International Data Corporation’s Project Magellan estimated costs at $320 billion worldwide, $134 billion of which was spent by the U.S.

[2] Some analysts also believe that other industrialized countries, such as the United Kingdom, Canada, Denmark, and the Netherlands, spent equivalent amounts per capita to the U.S.

The year 2038 is not expected to cause pervasive problems. The Y2K problem was generated by a widely used programming practice, whereas other problem dates are associated with limitations of software systems. Also, the sensationalism associated with Y2K heightened awareness of these other dates, so it is much less likely that future IT personnel will be surprised by date-related problems.

PROJECTED Y2K FAILURE TIMEFRAMES



Source: Gartner Group

Software that was remediated with a windowing approach or another similar technique utilizing two digits for representing a year may encounter problems with the approach of the "pivot year." A second problem may occur with systems that exchange year information in two-digit date formats but do not use the same pivot year. In addition, it is possible that remediated software will exhibit new problems. It is often the case that fixing one section of software causes new problems to occur (by introducing new defects elsewhere in the system).

In addition, during 2000 and beyond, government and private sector organizations must undertake permanent software fixes where temporary patches were utilized. Organizations may need to address non-mission critical systems where repairs were postponed. Internationally, most fixes were temporary clock rollbacks that ultimately must be fixed permanently.

The Committee thinks the most likely scenario will be problems with software that was not remediated at all for Y2K. These problems may show up in erroneous reports that are run at fixed times in the business cycle.

THE COMMITTEE'S CONTRIBUTIONS

Through tremendous efforts of the public and private sectors, the U.S. made a successful transition into the Year 2000. These efforts were propelled, in part, by a constant level of congressional attention to every aspect of the Y2K problem. This section summarizes the Committee's contributions to the nation's successful Y2K preparation effort.[3]

The Committee's mandate was to study the impact of the Y2K problem on the federal and state governments and the private sector, and to make appropriate findings of fact and recommendations to the Congress.[4] The Committee fulfilled this mandate by becoming a repository of information about the Y2K problem in order to focus public attention on the issue and spur action in the public and private sectors. The Committee accomplished this goal through the use of hearings, letters, regular interaction with public and private entities, reports, and legislative recommendations.

The Committee conducted 35 hearings on a wide array of Y2K issues (see Appendix III). Each hearing was designed to draw attention to a particular aspect of the Y2K problem; build general knowledge with regard to particular economic sectors; and elicit action to ensure a smooth transition into the Year 2000. Each hearing also served the critical function of educating the public about the nature and scope of the Y2K problem, and the ongoing progress of each sector. These numerous hearings kept pressure on the public and private sectors to remediate systems and to develop and implement contingency plans ensuring a successful Y2K event.

The Committee wrote hundreds of letters to various public and private entities to elicit information about Y2K preparedness and to encourage action. The letters also put these entities on notice that the Congress was exercising oversight with regard to Y2K. In the private sector, such letters helped shift the focus on Y2K from technical personnel to top management. This transition of responsibility was a crucial factor behind the success of the Y2K rollover. (Many of these letters were reproduced in Appendix II of the Committee's second report, "Investigating the Year 2000 Problem: The 100 Day Report.")

A crucial method of fact-finding was the Committee's regular interaction with representatives of the major federal agencies and critical private sector entities. This contact allowed the Committee to assess Y2K progress in all sectors, encourage the free flow of information, and maintain awareness of ongoing congressional oversight.

The Committee issued its first report, "Investigating the Impact of the Year 2000 Problem," in February 1999."[5]

[3] The Committee acknowledges the contributions made by numerous other Senate and House committees. The Committee also thanks the General Accounting Office (GAO), the investigative arm of the Congress, for the valuable assistance it provided in the form of reports, testimony, and other studies.

[4] S. Res. 208 (105th Cong., 2nd Sess.): To establish a special committee of the Senate to address the year 2000 technology problem, as amended by S. Res. 7 (106th Cong., 1st Sess.). The text of both resolutions can be found at Appendix II.

[5] S. Prt. 106-10, Feb. 24, 1999.

That report was the federal government's first comprehensive analysis of the nature and scope of the Y2K problem and the status of domestic preparations. The Committee issued its second report, "Investigating the Year 2000 Problem: The 100 Day Report,"[6] in September 1999. In addition to updating the first report, it contained an extensive analysis of international Y2K readiness. Both reports provided the public with a resource for understanding the problem and assessing its potential impact on the lives of American citizens and industries.

While the Committee was not granted legislative authority, it was tasked to provide legislative recommendations to the Congress, which it did on two occasions.

First, Senator Bennett introduced the Senate bill that would eventually result in the "Year 2000 Information and Readiness Disclosure Act," Pub. L. No. 105-271 (Oct. 19, 1998). This Act encouraged the disclosure and exchange of information about the Y2K problem by limiting the liability of companies that provided good-faith Y2K disclosures.

Second, Senator Dodd was instrumental in the passage of the "Y2K Act," Pub. L. No. 106-31 (July 20, 1999). This Act was intended to discourage the filing of frivolous lawsuits and to encourage parties to resolve Y2K problems prior to, and/or instead of, pursuing litigation.

Another vital aspect of the Committee's role was its bipartisan, cooperative approach toward a successful Y2K rollover. The committee and its members worked closely with House committees and with the President's Council on Year 2000 Conversion, as well as the federal agencies, private sector and international partners. The creation of successful public/private partnerships may serve as a model in the development of a national policy toward protecting American high-tech infrastructure.

[6] S. Prt. 106-31, Sept. 22, 1999.

LESSONS LEARNED/BENEFITS DERIVED FROM Y2K

Enduring lessons have been learned and benefits derived as a result of Y2K. There now exists a more thorough understanding of IT-related challenges, including effective quantification of IT problems and their probable impact. There is also a higher awareness of the integral role IT plays in business functions, and the effort involved to effectively manage ephemeral information and high-tech organizational assets.

As a result of Y2K, IT foundations and management mechanisms have been modernized. Critical infrastructure protection and other IT issues now rank higher among the mission priorities of corporate and government executives. In addition, new public/private partnerships and more effective avenues of communication—both domestically and internationally–have been created that will be beneficial in addressing future IT challenges.

MODERNIZED TECHNOLOGY BASE AND MANAGEMENT EFFICIENCY

The attention of executive-level personnel at vital stages of Y2K prioritizing, planning, and remediation has resulted in higher levels of accountability and reliability in IT management. For the first time—and at a critical juncture in the development of an IT-driven economy—private firms and public organizations have been forced to look critically at the role of IT assets and to manage them as mission-critical resources. Information systems, via strategic management, have graduated to the boardroom.

While many analysts predicted that Y2k preparation would sap budgets and productivity in 1998-1999, a large percentage of Y2K spending was earmarked in existing IT budgets and productivity continued to increase. The Department of Commerce stated in November 1999 that *"[s]ome of the Y2K spending may involve 'shifting forward' new, productive, software and hardware investments which would have occurred eventually, offsetting to some extent the drag on productivity."*[7] Given the cost overruns and delays that typically plague IT projects, it is significant that IT departments were forced to adopt strict timelines and strategies for simultaneously fixing multiple systems. The Y2K preparation process added discipline to IT management, and mandated a more holistic approach to solving problems in internal and external systems.

A central management decision that emerged during Y2K remediation was whether to modernize or scrap legacy systems. As a result, organi-

[7] "The Economics of Y2K and the Impact on the United States," U.S. Department of Commerce, Economics and Statistics Administration, Nov. 17, 1999, at vii.

zations such as the U.S. Postal Service have completely renovated information infrastructures.

Many organizations constrained to updating legacy systems have—at the very least—created system documentation for the first time, a step that will aid future IT problem-solving.

According to Committee testimony, many private firms and public agencies discovered during Y2K preparation that IT inventory was inaccurate or absent. Through a process of auditing, organizations learned that they were more vulnerable to problems in IT than previously believed.

BETTER COMMUNICATION NETWORKS AND PUBLIC/PRIVATE PARTNERSHIPS

The Y2K problem existed on such short timelines that a federal top-down regulatory approach was not practical, except within the existing framework of highly regulated industries. The financial sector was one such regulatory environment, while small chemical producers were not. Further, the constantly evolving status of compliance meant that most compliance information was out-of-date the moment it was published.

The challenge was to create networks of individuals, industries, and organizations to share information, and a legal environment where information could be readily shared. The Year 2000 Information and Readiness Disclosure Act provided relief from some antitrust concerns of intra-industry information sharing. The Y2K Act provided an additional incentive for vendor-initiated "due diligence" and corporate cooperation.

Trade associations were instrumental in the establishment of industry Y2K practice standards and in communicating results of compliance efforts. Such monitoring of the changing compliance environment created an incentive for organizations to avoid being the last across the finish line.

The use of the Internet was also a significant change in managing a potential national and global crisis. Nearly every business with a presence on the web had a link to a statement regarding Y2K compliance. Other web sites, such as that provided by the Food and Drug Administration, listed medical devices and linked to company compliance information.

Industry groups, associations of public managers, and trade organizations all established web sites that explained how a particular industry was Y2K ready, or how members could become Y2K compliant. As one computer industry spokesman noted, "*both companies and countries coming late to Y2K were able to gain enormous efficiencies from the shared experience of others. These efficiencies expressed themselves in saved work, fewer mistakes and false starts, more productive pro-*

cesses, a better understanding of available tools and supports, compliance information and more.”[8]

Use of the Internet provided an unprecedented level of organizational transparency. This transparency paved the way for effective public/private partnerships and open communication between different industries preparing for Y2K. Companies and industry groups employed aggressive methods of evaluating Y2K progress. For example, the telecommunications industry was evaluating the Y2K readiness of the power industry, the banking industry was evaluating the telecommunications industry, and the power industry was looking at both industries as sources of Y2K vulnerability. Once these groups began publishing readiness reports about each other, it became clear that insular perspectives were ultimately self-defeating, given the level of industry interdependence. As Howard Rubin testified before the Committee, “[m]*ore recently, a major shift in the global position and posture with regard to Year 2000 has to do with the realization of the level of interaction between and within nations and sectors*.“[9]

KEY PRIVATE/PUBLIC PARTNERSHIPS

Sector	**Trade Association**	**Lead Federal Organization**
Airlines	Air Transport Association	Department of Transportation
Electric Power	North American Electric Reliability	Department of Energy
Financial Services	Securities Industry Association	Securities and Exchange Commission
Natural Gas	American Gas Association Interstate Natural Gas Association of America	Department of Energy
Oil	American Petroleum Institute	Department of Energy
Pharmaceuticals	National Pharmaceutical Alliance National Association of Chain Drug Stores	Department of Health and Human Service
Retail	National Retail Federation	Information Coordination Center
Telecommunications	Network Reliability and Interoperability Council	National Communications System

The President’s Y2K Conversion Council deserves an enormous amount of credit for facilitating public/private partnerships. Key partnerships are shown in the table. By establishing more than 20 sector working groups chaired by a federal agency, with private sector trade association participation, much sharing of information and cross sector coordination was made possible. This sharing of lessons learned enabled work to be completed more effi-

[8] Testimony of Harris Miller, President of the Information Technology Association of America, before the Subcommittee on Government Management, Information, and Technology, House Committee on Government Reform and Oversight, January 27, 2000.

[9] Testimony before the Senate Special Committee on the Year 2000 Technology Problem, October 13, 1999.

ciently than would otherwise have been possible, and provided a level of comfort among dependent sectors that specific Y2K concerns were being addressed. The Committee finds that these private/public partnerships may be useful for addressing computer security, infrastructure protection, and other IT issues in the future.

Useful partnerships were also established internationally. Many international organizations were instrumental in heightening worldwide Y2K awareness and in stimulating action. Most importantly, the United Nations (UN) held its first Y2K event in December 1998. About 120 countries sent delegates and, according to John Koskinen, "*probably half of whom weren't sure why they were there*."[10] By the UN's second meeting in June 1999, where more than 170 countries sent delegates, nearly all had mounted a serious national effort to ensure their critical systems would be ready.

The International Y2K Cooperation Center was established in February 1999 under the auspices of the UN with funding from the World Bank. This organization created a useful mechanism for governments from member countries to share information and lessons learned about Y2K. the Cooperation Center probably enabled countries, particularly those that got off to a slow start, to catch up by more efficiently addressing Y2K problems. Although the Center is scheduled to disband on March 1, 2000, the Committee finds that some type of similar international coordination mechanism could be useful in addressing future IT issues.

GREATER AWARENESS OF IT DEPENDENCIES & SECURITY RISKS

Y2K prompted the government and the private sector to closely examine the IT infrastructure upon which they had come to rely. As contractors and subcontractors were brought in to do inventory assessments and to test and remediate software and hardware, many organizations began to think carefully about the risk to information security. To varying degrees, the entire business enterprise of virtually every private organization and government entity has been opened to outsiders.

As the Committee noted in its 100 Day Report, the risk of giving outsiders sudden access to systems that once belonged only to trusted insiders presents a credible risk to information security stability. The GAO recently criticized the Federal Aviation Administration for giving non-U.S. citizens access to highly sensitive information systems critical to air safety.[11] Currently, the breach to security remains unknown.

[10] Testimony before the Subcommittee on Government Management, Information, and Technology, House Committee on Government Reform and Oversight, January 27, 2000.

[11] "Computer Security: FAA Needs to Improve Controls Over the Use of Foreign Nationals to Remediate and Review Software," AIMD-00-55, Dec. 23, 1999.

There is no geography in the world of software. Y2K corrections were made around the world with tremendous speed, and a variety of fixes were implemented. There is some degree of risk associated with the rapid deconstruction of successful Y2K programs and the dispersal of the system expertise that was developed.

Security is a process of becoming, not a state of being. The e-commerce revolution has perforated complex interconnected business entities with security breaches. Information technology and security issues have moved from the backroom to the boardroom. The communities that most need to be engaged are financial analysts, who can drive the business to excel at information security.

The need to shore up information security was reinforced by the wave of denial of service attacks that occurred during the first weeks of February 2000. Such attacks raised questions about the security of web sites used by millions of Americans for both pleasure and business. The threat to these businesses should provide additional incentive to the industry to work together with government to form a united front against future attacks.

Perhaps Y2K has helped organizations develop a keener sense of their dependency on information technology. Before Y2K occurred, the DOD did not know how many mission-critical systems it had. Likewise, many corporations found that they were not aware of the redundancy or the inefficiency of their information enterprises.

Y2K significantly raised the importance of IT issues and caused much of government and industry to raise security and reliability as top executive priorities—a position they will likely maintain for the foreseeable future. A great deal of attention has been given to securing the Internet and making transactions for e-commerce safe and trusted. However, the question remains whether the requisite attention has been given to the assurance and security of the Internet infrastructure.

WHAT'S NEXT/HOW DO WE CAPITALIZE ON Y2K?

Y2K has heightened awareness about the importance of high-tech infrastructure protection. Since its formation, the Committee has focused closely on technological vulnerabilities in key national infrastructures.

It is the Committee's assessment that improving critical infrastructure protection will be the next major challenge to the IT community. The Senate must examine congressional structure and efficacy for addressing critical infrastructure protection and future IT issues.

MAINTAIN/ENHANCE Y2K NETWORKS AND PUBLIC/PRIVATE PARTNERSHIPS

During the readiness process, new relationships and partnerships were forged to combat the shared risk of Y2K vulnerability. The interconnectedness and interdependencies of modern businesses and organizations, across all industry sectors, required that programs addressing Y2K not simply focus internally, but also on supply chain relationships and business partnerships.

In the Information Age, the relationships established for Y2K will prove invaluable. Many of the efforts undertaken to manage and remedy the Year 2000 problem can also be applied to long-term challenges. For example, the challenge of protecting critical infrastructures from computer-based attacks extends well beyond federal operations. It spans the entire spectrum of the national and global economies.

Many critical infrastructure facilities are owned and operated by private companies whose continued secure operations are essential to the national welfare. As a result, establishing public-private partnerships has been recognized as one of the major challenges of critical infrastructure protection.

Year 2000 preparation addressed numerous vulnerabilities outside the federal government. Vulnerabilities were identified in state and local governments, the public infrastructure, and other key economic sectors such as financial services. A single failure in one system could affect many others, including those in the nation's complex array of public and private enterprises that have system interdependencies at all levels.

For this reason, it is important that domestic and international industry and government partnerships nurtured during Y2K preparations are maintained and continue to grow.

LEVERAGE Y2K LESSONS TO IMPROVE INFRASTRUCTURE PROTECTION

Preparation for Y2K prompted a significant, worldwide investment in business information systems and high-tech infrastructures. This investment has not only improved system and network reliability, but has also accelerated e-commerce and globalization. Globalization—rapid economic, technological, cultural and political integration—is bringing citizens from all continents closer together, allowing them to instantaneously share ideas, goods, and information. The Internet, globalization's superhighway, has become an essential tool for strategic coordination and communication in government and private industry.

With its rewards, however, globalization also brings risks. Aside from the traditional threats associated with weapons of mass destruction, terrorism, drug trafficking, and other international crimes are global concerns that transcend national borders.

Domestic national security and economic strength is no longer protected by geographic separation from adversaries by the Atlantic and Pacific oceans. The new geography of worldwide Internet connectivity leaves the U.S. vulnerable to the impact of economic problems experienced in other countries, anywhere in the world.

In addition, the low cost and availability of computer technology places adversaries within a few keystrokes of key national systems. The interconnectivity and public access to U.S. information systems makes the nation more vulnerable to information attacks than most.

A looming challenge for U.S. policy makers lies in devising methods to detect, deter and respond to information attacks against critical national infrastructures.

Congress became concerned about information attacks and tasked the Administration to investigate, report and develop a plan for information and cyber defense 1996 and 1997. Presidential Decision Directive No. 63 (PDD 63) was issued in May 1998, and a national plan for critical infrastructure protection was released in January 2000. These documents constituted the federal government's first formal approach to national defense against information-based attacks.

The National Security Strategy released by the White House in January 2000 outlines the issues of vital interest to the country. Among these are the physical security of the U.S. and its allies, the safety of U.S. citizens, the economic well-being of American society, and the protection of our critical infrastructures, such as energy, banking and finance, telecommunications, transportation, water systems, and emergency services.[12]

The National Plan to protect information systems is entitled "An Invitation to Dialogue." Congress and the Administration must examine the following:

- The role of the DOD in providing a defense against information attacks;

- The U.S. definition of an information attack;

- The adequacy of organization and funding among the intelligence community to assess and address information warfare threats;

- The need for the National Intelligence Council to have an Information operations officer;

- A national security amendment to the Telecommunications Act of 1996 to outline a reconstitution requirement for Internet service providers; and

- A legal framework providing for the common defense while ensuring individual privacy and security.

The security challenges which will face the U.S. in the coming years will be increasingly complex. This is particularly so because the challenges are likely to be a mixture of physical and information-based attacks that tangle jurisdictional boundaries and thwart the timely response of the federal agencies.

CONGRESSIONAL ROLE IN INFRASTRUCTURE PROTECTION

Critical infrastructure protection includes a vast range of issue areas. Such areas include information and communications; banking and finance; water supply; transportation; emergency law enforcement; emergency fire service; emergency medicine; electric power, oil, and gas supply and distribution; law enforcement and internal security; intelligence; foreign affairs; and national defense. These activities cross multiple committee jurisdictions. Many congressional committees have oversight over small segments of critical infrastructure protection, and no congressional committee has the jurisdiction over the issue as a whole.

[12] “National Plan for Information Systems Protection Version 1.0: An Invitation to a Dialogue.”

[page left intentionally blank]

APPENDIX I

COMMITTEE ENABLING LEGISLATION

The Committee was established during the second session of the 105th Congress by Senate Resolution No. 208. This resolution, which was agreed to on April 2, 1998, set forth the Committee's purposes, membership, authority, and funding. Senate Resolution No. 208 was amended during the first session of the 106th Congress by Senate Resolution No. 7. This resolution, which was agreed to on March 2, 1999, increased the Committee's funding. The full text of both resolutions follows.

Senate Resolution 208, authorizing the Committee is available online at the Library of Congress *http://thomas.loc.gov/*.

http://thomas.loc.gov/cgi-bin/query/z?c105:S.RES.208:

Senate Resolution 208, authorizing the Committee is available online at the Library of Congress *http://thomas.loc.gov/*.

http://thomas.loc.gov/cgi-bin/query/z?c105:S.RES.208:

Senate Resolution 208, authorizing the Committee is available online at the Library of Congress *http://thomas.loc.gov/*.

http://thomas.loc.gov/cgi-bin/query/z?c105:S.RES.208:

Senate Resolution 208, authorizing the Committee is available online at the Library of Congress *http://thomas.loc.gov/*.

http://thomas.loc.gov/cgi-bin/query/z?c105:S.RES.208:

Senate Resolution 208, authorizing the Committee is available online at the Library of Congress *http://thomas.loc.gov/*.

http://thomas.loc.gov/cgi-bin/query/z?c105:S.RES.208:

Senate Resolution 208, authorizing the Committee is available online at the Library of Congress http://thomas.loc.gov/.

http://thomas.loc.gov/cgi-bin/query/z?c105:S.RES.208:

Senate Resolution 208, authorizing the Committee is available online at the Library of Congress *http://thomas.loc.gov/*.

http://thomas.loc.gov/cgi-bin/query/z?c105:S.RES.208:

Senate Resolution 208, authorizing the Committee is available online at the Library of Congress *http://thomas.loc.gov/*.

http://thomas.loc.gov/cgi-bin/query/z?c105:S.RES.208:

Senate Resolution 208, authorizing the Committee is available online at the Library of Congress *http://thomas.loc.gov/*.

http://thomas.loc.gov/cgi-bin/query/z?c105:S.RES.208:

APPENDIX II

EXAMPLES OF Y2K GLITCHES

The full extent of Y2K problems will probably never be known because only a small fraction of the actual occurrences will be reported. There is no incentive for corporations or countries of the world to openly report computer problems. As with any internal problems, organizations will likely simply fix them and continue their operations unbeknownst to the general public. The problems listed below were compiled from a variety of public and private sources including news services. While the sources are considered to be reliable, the Committee was not able to verify each incident or specifically attribute it to Y2K.

Utilities:

- Several electric utilities in North America have reported minor glitches with the synchronization feature of the clocks used in their energy management system computers
- Seven nuclear power plants experienced minor Y2K glitches in non-safety systems and were quickly fixed
- Hadley, MA: Software used to process data and create reports at the town's wastewater treatment plant has experienced a Y2K failure
- Hundreds of Knoxville Utilities Board bills were printed with incorrect "payment due" dates, either in January 1900 or January 2099.
- The new Manatee County Public Works system was spitting out water, sewer and garbage bills with unrelated and incorrect data, but corrected utility bills are finally in the mail for 20,000 Manatee County (Florida) customers a month late after changes intended as Y2K fixes caused problems
- A power outage in Carson City, Nevada for 30 minutes
- Santa Fe water company experienced billing system glitches
- Akron, Ohio water company sends out erroneous shut off notices to 3000 customers
- Grand Prairie,

Healthcare:

- Tissue processor medical device in VA hospital would not accept 2000 as a date to run on automatic, but would operate manually
- Medical displays of Sera-520 model electrolysis analyzers have incorrect date stamp, but operation not affected

- Florida and Kentucky reported Y2K-related problems with their unemployment benefits' automated telephone call processing system. 100 claimants in Florida and fewer than 50 claimants in Kentucky were effected and the problems were fixed
- Guam implemented manual processing for several welfare systems that were not Y2K compliant
- $50 million in Medicare payments were delayed 1 day because of a Y2K problem with the electronic fund transfer through a bank that handles such transactions
- Medicare provider claims are being returned (rejected) because they are being submitted with dates of 1900 or 2099. One contractor alone had received about 11,000 claims with these erroneous dates
- Oregon had Y2K-related errors in systems used for Food Stamps, Child Support Enforcement, and Temporary Assistance for Needy Families. The problems were fixed, but a 1 day delay in some payments to clients resulted

Telecommunications:

- Charlotte, North Carolina: 911 systems broke down Wednesday 12/29/99 during rounds of Y2K testing
- Emergency telephones along Interstate 87 stop working
- Long distance phone service was out in widespread parts of central Montana for about three hours
- Cisco issues notices of router problems since rollover and for February 29
- 911 problems in Orange County Florida
- 911 system in the Minneapolis metro area experienced problems on January 30th for several hours due to a system upgrade.

Transportation:

- Amtrak's Philadelphia Control Center system would not retain train symbols as the train progressed on the system
- Two key FAA systems experienced Y2K problems that were quickly resolved: (1) the Low Level Wind Shear Alert System at eight sites, (2) Kavouras Graphic Weather Display System
- Power Conditioning System Data terminal equipment in four cities displayed the date "1900" on rollover
- ARINC Oceanic Display and Planning System printers in two locations failed the transition from 1999 to 2000. These are not FAA printers but are a redundant system used in the relay of data from ARINC communications centers to air traffic controllers handling oceanic traffic
- I n Chicago, an airport wind-shear alert system had a minor glitch that flashed an error message at four smaller airports and railroad gates in Shiloh went down without reason and stayed down

Financial:

- Bank credit card companies reported problems with merchants who did not install free upgrades to CyberCash, Inc. software; result was duplicate postings of charges
- Federal Reserve Bank of Chicago reported glitch in transferring tax payments from customers of 60 financial institutions
- Failure of overnight batch credit card settlement through Chase Merchant Services

General Business:

- Godiva Chocolates (parent company – Cambell Soup) experienced total systems failure including cash registers in its New York store, but were back in operation within three hours.
- Several news papers find problems with dates in online editions, but content was not affected
- A small Portland trucking firm could not access any of its accounting information as a result of not installing upgrades to its BizWorks software
- Incorrect dates appeared on office automation software for a small New Jersey trucking firm, but did not impact operations
- Retailers that did not update their ICVerify systems could not do batch settlements after close of business; did not affect customer transactions, but could affect thousands of small businesses
- Department of Defense Satellite-based intelligence system experienced a Y2K failure shortly after GMT in the ground station
- The District of Columbia replaced its non-Y2K compliant system with a new financial management system late last year – & delays in full implementation are expected to delay some budget reports
- Some driver licenses issued by the state of Indiana contained an incorrect expiration date due to a Y2K glitch. According to the Indiana Bureau of Motor Vehicles, "Persons under age 75 received a driver license that expires in 2005, although state law mandates that a license is valid for four years. Motorists age 75 and older are required to renew a driver license every three years, but licenses issued since Jan 2 show an expiration date of 2004."
- A Y2K problem caused Richland, Mississippi police dept. to sent out hundreds of incorrect letters demanding immediate payment for traffic fines, some of which had already been paid
- The Navajo Nation Law Enforcement reported that seven of its eight computer-aided dispatch servers failed and a manual process was used until the servers were fixed on January 19, 2000
- The security access system froze in an open position due to malfunction in clock system in a federal building in Omaha

- Computers in three Hampstead county (Arkansas) offices have been bitten by the Y2K bug. The glitch in the program has halted work on payroll and claims
- In Chicago, the city's Doppler radar system went down for about five minutes.
- A computer-run energy-management system at a federal building in Chicago suddenly flashed the date Jan. 4, 1980
- Redmond, Washington experienced problems with its city-issued fuel access cards, and the police department's computer-aided dispatch system found a minor Y2K bug

General Government:

- 800 slot machines in Delaware shut down after reading the current date as January 1, 1900
- Highland Bank of Chicago experienced problems receiving and processing electronic funds transfer payment files affecting a Medicare contractor in California, Oregon, Arizona, and New York
- Florida and Kentucky reported problems with unemployment insurance benefit systems that delayed individuals from filing claims
- The Y2K bug caused a few minor malfunctions in Apple Computer Inc.’s information technology system.
- Slot machines malfunctioned on December 31st due to Y2K
- U.S. Homecare had to create manual work-arounds for all basic functions, from billing to payroll because of Y2K glitches that struck shortly after the new year
- Lamonts Apparel Inc., which operates 38 department stores in the Pacific Northwest, filed for Chapter 11 bankruptcy protection. The company said that its cash flow had been squeezed by slow spring and summer sales and unexpected costs associated with fixing its Y2K computer problems The company paid a combined $10 million to install new computerized registers and other hardware as part of its efforts to combat the Y2K bug
- The government listings in the Milwaukee white pages are so riddled with errors that Ameritech Corp. has agreed to reprint that section and hand-deliver it for free to consumers next month. The company updated its software last year to make it Y2K-compliant. But the software had bugs and introduced the errors into the system
- In Champaign, Ill., roughly 8,500 Illicall subscribers received their January 2000 long-distance statements; however, they appear to be a century old already because of a Y2K glitch

International:

Australia

- Telephone outages in southern Australia
- Payroll calculated from 1900 at Sybiz Software

- PC problems reported by Microsoft Australia
- Electric train ticket sales equipment in Sydney registered wrong date
- Public transport ticketing system failed in Tasmania and South Australia

Austria

- City of Vienna EDP systems failures

Belarus

- Pension payment system problems

Benin

- Bank pension systems malfunction
- Telecommunications switching problems
- Maritime GPS equipment malfunction
- Train telecommunication switch disruptions

Bolivia

- Failure in a customs system at Puetro Suarez
- Land property registration glitches
- Minor glitches at a public office in Cobija
- Health diagnosis equipment failure
- Accounting software (SINCOM) failure

Botswana

- Fax and telex system failures within government offices
- Medical equipment failures at Athlope Hospital
- Police department fax and telex system problems

Brazil

- Airport customs systems did not recognize receipts issued last year
- Port customs system did not recognize receipts issued last year
- Convenience store cash registers could not process receipts
- Hospital appointment system failed
- Toll booths unable to process receipts

Bulgaria

- Internet servers unavailable shortly after rollover

Canada

- Public school system payroll miscalculations
- Prison door systems failed in British Colombia
- Department of motor vehicle system malfunction
- Failure of a switching station in Oshawa
- Malfunctions on individual portfolios on the Toronto Stock Exchange website

China

- A few mid- to small-businesses" financial systems failed
- A QingDao hotel reported a problem in its control system for room assignments
- Taxi meter failures reported in NanJing
- ATMs would not dispense cash and had incorrect balance displays
- Database problems at the Anning Printing Plant

- Savings bank electronic time keeping board malfunctions
- Reporting/query system malfunctions at newspaper offices
- Date display malfunctions at Sino-Japanese Friendship Hospital
- Halian Department Store system malfunctions
- State Meteorological Administration computerizxed monitoring system failed
- Peoples Bank internal and interbank e-mail and credit card system failures
- Taxi meter failures

Colombia

- Social security systems date validation conflicts
- Non-compliant maritime tank ship

Costa Rica

- Billing system problems at a petroleum refinery

Czech Republic

- Taxi meter failures
- Land registry office system malfunctions

Denmark

- Second largest bank, UNIBANK, identified glitch in Unitel payment and information systems for about 20 corporate clients

Ecuador

- Internet server problems at the Ministry of Labor
- System malfunctions at the offices of the Attorney General

Egypt

- Hospital dialysis machine failures

France

- Ground station communication problem relating to Syracuse II satellite
- Finance, personnel, and production system malfunctions at more than 15% of the nation’s small businesses

Gabon

- Isolate incidents with some accounting systems

Gambia

- Miscellaneous air and sea transportation system failures
- Custom service system failures
- Miscellaneous tax service system failures
- Unspecified power outages
- Miscellaneous treasury department system failures

Germany

- Cash register failures
- Berlin’s German Opera experienced payroll system anomolies
- Cologne Bank on-line banking glitches

Ghana

- Bio-medical equipment malfunctions at the Korle Bu Teaching Hospital
- Telecommunications phone line malfunctions
- Power system billing and equipment problems at the Dolta River Authority

Greece

- Problems with older model cash registers
- Billing system date anomalies at Athens utility

Grenada

- Manual backup used in lieu of compliant customs service computer system
- Payroll component of the National Water and Sewerage Authority, the sole provider of water in Grenada, was not compliant

Guatemala

- Miscellaneous system failures reported by several medium and small enterprises

Hong Kong

- A local area network used by a training department contained incorrect date field
- Instruments used by police department to conduct breathalyzer tests failed, but were fixed within 10 days
- Improper calculations in Hong Kong Futures Exchange's options pricing system
- Hospital blood sample analyzer equipment date stamp problems
- Office automation problems within the Agriculture and Fisheries Department
- Miscellaneous glitches reported by about 10 small businesses

Indonesia

- Bank of Indonesia command center computer malfunctions
- Bank Niaga ATMs deny access to customers
- Mobile phone billing system failures

Iran

- Blood gas analyzer failed in a Tabriz hospital

Iraq

- Oil export pipeline system clock rolled back

Ireland

- Eircom's automated balance system displayed incorrect date

Israel

- Miscellaneous minor problems reported by Defense, public and government institutions and banks

Italy

- Automated systems use by Naples and Venice courthouses failed
- Bari Central Court system inadvertently erased 1999 data
- Miscellaneous problems reported by 20 small town governments
- Electro medical equipment malfunctions
- Time card machines malfunction
- Telecom Italia signaling and billing system anomalies

Jamaica

- 8 traffic lights (30% of Corporate Area) went out

Japan

- Weather monitoring and reporting system non power related problems at Shika Nuclear Power Plant
- Glitch in a system used to provide weather information for small airplanes
- Japanese Railway ticket distributing system problems
- Japanese electronics firms experienced 50 different problems in various business and plant computer systems
- Bicycle parking lot machines malfunction
- Fire and emergency systems failures
- Government vehicle tax computers malfunctioned
- Government residency computers malfunctioned
- JR Sakaide Station entrance gate system did not recognize employee passes
- Noise monitoring system at New Tokyo International Airport lost data
- Tokushima University's bone density measuring device miscalculated patient ages
- Sewage works device malfunction
- NTT Mobil Communications phones deleted messages
- Matsushita Communications registered mail software malfunctioned
- IDO Corp. mobile phones do not display dates
- Hokuriku Electric Power Company's emergency data transmission system malfunctions
- Tokyo Electric Power Company experience problems in data storage and processing systems, detectors, position control rods, and test radiation analysis system
- Toyota Motor Company navigation devices malfunction
- 10 banks and credit cooperatives experienced bankbook date and ATM data display problems
- Onagawa Nuclear Plant electric substation failure
- Rokkashomura Nuclear Waste Storage Facility management and monitoring system date malfunction
- 12 small brokerages experience glitches in record keeping systems
- Tokyo Stock Exchange experienced errors in back office system
- Tohoku Electric Power Co. jauge to measure sea water problems failed

Kazakhstan

- Manual operation employed to overcome computer system problems at Ekibastuz Hydroelectric Power Station-@
- Kazakh Railway Co. personal computer problems
- Systems used to control air conditioning and elevators in government buildings failed because Johnson Control Company upgrades not installed

Latvia

- Incorrect date stamps on systems at Riga City customs office

Malawi

- Hotel booking system failed and lost registrations

Malaysia

- Failure of a building automation system at the Sibuand Muar Hospitals
- CTG machine at Tung Shin Hospital experienced date stamp problem, but continued to operate
- Failure of patient registration system at Machang Hospital
- Ultrasound machines at Sultanah Aminah and Muar Hospitals experienced date problems
- Blood gas analyzer at Alor Setar Hospital had date stamp problem
- Blood Pressure monitor at Bintulu Hospital had date stamp problem
- Several land offices experienced problems in billing system software
- Several gas pump display panels displayed wrong dates
- Penang province satellite television went out

Mali

- Systems used to monitor the transport of merchandise and dispense tickets for a Mali ferry systems broke down

Mexico

- Some medical equipment such as ultrasound, X-ray, and clinical analysis machines experienced date stamp problems

Moldova

- Transports and Communications Ministry experiences date malfunctions

Mongolia

- A few railroad ticketing systems experienced problems, but were fixed the same day

Namibia

- Database used by Ministry of Works, Transport, and Communication did not correctly recognize year 2000 dates
- Channel 7 radio station’s advertising scheduling system failed; manual operations were employed
- Bank of Namibia ATMs had difficulty detecting bar codes

Netherlands

- Miscellaneous failures in on-line banking systems

New Zealand

- Mobile computer units in ambulances failed
- Auckland University database could not be reset
- Unspecified water pumping station problems
- Miscellaneous minor power outages in Invercargill and Alexandria
- Police computer system outage
- Air traffic control system radars were operating, but inter connections were down
- Bus pass validating machines would not accept passes
- Auckland Airport website date anomalies

Nicaragua

- Minor glitches reported by Supreme Court and Ministry of Agriculture
- Date problems in ultrasound and dialysis machines reported by Ministry of

Health

- Unconfirmed reports of glitches in 800 medium sized companies
- Nueve Segovia Local System of Integral Health Statistics failed
- Ministry of Agricultural Development and Forestry reported miscellaneous system failures

Nigeria

- Port Harcourt refinery maintenance and material management system problems was fixed within 3 hours
- Non-compliant telephone companies were intentionally disconnected to avoid problems

Norway

- Cash register failures at 7-Eleven stores
- Isolated ATM failures
- Hospital X-ray machines malfunction

Pakistan

- Computer system malfunction at the Karachi Development Authority
- Electric power authority experienced cascading failures in transmission lines in Multan, Faisalabad, Tarbela, and Mangla
- Date malfunctions at the Islamabad Stock Exchange

Palestinian Authority

- Miscellaneous failures in government systems

Philippines

- Several date stamp problems reported in fax machines and other non-critical electronic equipment
- Philippine Rural Bank declared holiday to curtail massive cash withdrawals

Portugal

- Minor Y2K glitches in hospital payment and admissions systems
- Miscellaneous problems with government Ministerial databases and payment processing systems

Republic of Korea

- Heat and hot water loss in an apartment building
- Medical device used for density measurement failed
- Various problems at an aluminum manufacturing plant

Russia

- Nuclear power plant management system malfunctions
- Government system e-mail disruptions
- Telephone switch failure in the central Sverdlovsk region and the city of Orenburg
- Boiler pump failure caused 8900 people in the far east to lose heat
- Operational control system malfunction in Lenergo Power's central control room

Rwanda

- Operating system for customs computer failed

Saudi Arabia

- Medical equipment such as electrocardiogram, ultrasound and arterial blood gas machines experienced date function problems
- Locally designed software had problems in comparing Muslim to western dates
- University student transcript system anomalies

Slovakia

- Incorrect date displayed on bank webpage
- Incorrect date displayed on weekly magazine webpage
- Hydrometeorological Institute system malfunctions

South Korea

- Graduate certificates dated 1900 at Korea University
- Video rental store computers could not accept 2000 dates
- Hotel reservation systems malfunction
- Production control data exchange problems at Ch'angwon Industrial Complex aluminum manufacturing plant
- Bone marrow equipment and patient registration systems malfunctioned at Ansan Severance Hospital and Dongshin Hospital
- Automatic broadcast system failed at Bukshim Cable TV requiring manual intervention
- Apartment building heat and hot water system failures
- Trial summons dated 1900 at Provincial Court

Spain

- Two nuclear power stations reported problems with non-critical computer systems

Sri Lanka

- A Holter ECG Monitoring Units failed at Shri Jayawardenepura Hospital
- Blood gas analyzers and intensive care unit equipment failed at Kandy Hospital
- Supermarket point of sale electronic funds transfer system malfunctioned

Sudan

- Interbank communications in two banks delayed by two days

Sweden

- Isolated glitches in healthcare and hospital admissions systems
- Parking meter problems
- Cash register failures
- Computerized entry to sport center not working
- Control and surveillance system problems in a water plant
- Hospitals experienced problems with kidney dialysis equipment and electrocardiograph machines
- Ikea store card system rejected cards as out of date
- 10% of customers report internet banking problems

Taiwan

- Blood pressure measuring machine and hospital registration problems in Taoyuan County

Tajikistan

- Miscellaneous government computer system failures

Tanzania

- Zanzibar reported television transmission problems

Thailand

- Meteorological Department satellite date anomalies
- Unspecified computer system failures at Loei Hospital
- Power plant date malfunctions
- Analysis tool displayed erroneous date at Rama Hospital
- Tele-banking and cash management system data feed problems at Siam Commercial bank

Turkey

- Minor glitches reported in biomedical equipment at a few hospitals including blood sample analyzing machines, patient monitoring equipment, ultrasonic devices, tomography devices and dialyses machines
- Miscellaneous Y2K glitches experienced by several manufacturing companies including Akin Tekstil, Arcelik, Emsan Besyildiz, Emsan Paslanmaz, and Erciyas Biracilik

Uganda

- Non-compliant computers at examinations authority forced manual work-arounds
- Nakawa Inland Port billing system failure
- Education facility’s academic test processing system required manual work-around

Ukraine

- Nuclear power plant system failure caused a 45% reduction in power generation

United Kingdom

- Welsh Tax Office had forms dated 1900 returned
- English Registry Office system erroneously recorded 1900 on birth certificates
- Surveys show that about 5% of private firms experienced computer failures
- Sainsbury Superstore had point of sale equipment failures
- Two nuclear power stations had malfunctions in monitoring systems and data transfers
- Date malfunctions at the Oldham Chronicle’s website
- BBC had unspecified system malfunctions
- Accounting systems malfunction at the Portman Building Society
- Racal/HSBC point-of-sale terminals would not accept cards

Venezuela

- Shutdown of biomedical equipment laboratory analyzer optic reader
- Temperature monitoring system at a major aluminum manufacturing facility

shutdown and required manual intervention to sustain operations

Vietnam

- Isolated telephone switching problems
- Small and medium sized enterprises experienced problems with Novell Netware 4.1 operating system

Zambia

- Telecommunications interruptions between Zambia and Malawi
- Financial management system software used by all government ministries experienced problems that caused incorrect calculations

Zimbabwe

- City of Harare's financial system failed causing delays in billings for water
- Town of Ruwa reported that their financial and billing system went down
- Central Mechanical Equipment Department's computer system crashed
- Ministry of Mines experienced office automation problems

APPENDIX III

COMMITTEE HEARINGS

106th Congress

12/08/99:	“Y2K: Will Our Seniors Suffer?” (Field Hearing)
10/25/99:	“Y2K’s Impact on the Economy” (Field Hearing)
10/22/99:	“McDonald’s: Is the Largest ‘Small Business’ Y2K Ready?”
10/13/99:	“International Preparedness: What in the World Will Happen?”
10/07/99:	“’Virtual’ Hearing on Emergency Preparedness”
09/30/99:	“Will Y2K Snarl Global Transportation?”
09/28/99:	“Y2K and Russia: Potential Impacts and Future Consequences?”
09/21/99:	“Education and Y2K: Will Our Schools Make the Grade?”
08/04/99:	“Y2K Update on Gas and Electric Utilities” (Virtual Hearing)
07/29/99:	“Y2K Response, Recovery, and Cyber-Reconstitution: Understanding the Role of the Information Coordination Center”
07/22/99:	“The Year 2000 and Global Corporations: Will the Bug Bite Big Business?”
07/15/99:	“State and Local Government Year 2000 Preparedness”
06/22/99:	“Federal Y2K Spending: Where is the Money Going?” (Joint Hearing with the Senate Appropriations Committee) (S. Hrg. 106-219)
06/10/99:	“Y2K and Healthcare: It’s Time for Triage”
05/25/99:	“Community Y2K Preparedness: Is There News They Can Use?”
05/10/99:	“Will Y2K and Chemicals be a Volatile Mix?” (Field Hearing) (S. Hrg. 106-160)
04/29/99:	“911 and Y2K: Will the Call be Answered?” (S. Hrg. 106-186)
04/22/99:	“Year 2000 and Oil Imports: Can Y2K Bring Back the Gas Lines?”
04/14/99:	“Federal Government Year 2000 Preparedness: What’s Next for Those Who Missed the March Deadline?”
03/30/99:	“Y2K in Nevada” (Field Hearing)
03/11/99:	“Y2K in the Courts: Will We Be Capsized by a Wave of Litigation?” (S. Hrg. 106-97)
03/05/99:	“International Year 2000 Issues: Will the World Be Ready?”
03/02/99:	“The Food Industry and Y2K: Starving for Attention?” (S. Hrg. 106-38)
02/19/99:	“The Millennium Bug: Is Oregon Prepared?” (Field Hearing) (S. Hrg. 106-88)
02/05/99:	“The Food Supply: Will the Cupboards be Bare?” (S. Hrg. 106-89)

105th Congress

12/18/98: “Y2K + H20: Safeguarding Our Most Vital Resource” (S. Hrg. 105-971)
10/07/98: “Small Businesses to Global Corporations: Will They Survive the Year 2000?” (S. Hrg. 105-894)
10/02/98: “Emergency Planning for the Year 2000: Preparation or Panic?” (S. Hrg. 105-895)
09/17/98: “The Year 2000 Technology Problem: Pensions and Mutual Funds” (S. Hrg. 105-770)
09/10/98: “Transportation After Y2K: Can We Get There From Here?” (S. Hrg. 105-777)
07/31/98: “Telecommunications and Y2K: Communicating the Challenge of the Year 2000” (S. Hrg. 105-692)
07/23/98: “The Year 2000 Computer Problem: Will the Health Care Industry Be Ready?” (S. Hrg. 105-688)
07/06/98: “International Banking & Finance: An American Perspective” (S. Hrg. 105-628)
07/01/98: “Northwest Year 2000 Summit” (Field Hearing) (S. Hrg. 105-693)
06/12/98: “Utilities and the National Power Grid” (S. Hrg. 105-617)