

105TH CONGRESS }
2d Session }

COMMITTEE PRINT

{ WMCP:
105-10 }

SUBCOMMITTEE ON OVERSIGHT
OF THE
COMMITTEE ON WAYS AND MEANS
U.S. HOUSE OF REPRESENTATIVES

REPORT
ON
THE YEAR 2000 COMPUTER PROBLEM



AUGUST 19, 1998

Prepared for the use of Members of the Committee on Ways and Means
by members of its staff. This document has not been officially approved
by the Committee and may not reflect the views of its Members

U.S. GOVERNMENT PRINTING OFFICE

50-311 CC

WASHINGTON : 1998

COMMITTEE ON WAYS AND MEANS

BILL ARCHER, Texas, *Chairman*

PHILIP M. CRANE, Illinois	CHARLES B. RANGEL, New York
BILL THOMAS, California	FORTNEY PETE STARK, California
E. CLAY SHAW, JR., Florida	ROBERT T. MATSUI, California
NANCY L. JOHNSON, Connecticut	BARBARA B. KENNELLY, Connecticut
JIM BUNNING, Kentucky	WILLIAM J. COYNE, Pennsylvania
AMO HOUGHTON, New York	SANDER M. LEVIN, Michigan
WALLY HERGER, California	BENJAMIN L. CARDIN, Maryland
JIM McCRERY, Louisiana	JIM McDERMOTT, Washington
DAVE CAMP, Michigan	GERALD D. KLECZKA, Wisconsin
JIM RAMSTAD, Minnesota	JOHN LEWIS, Georgia
JIM NUSSLE, Iowa	RICHARD E. NEAL, Massachusetts
SAM JOHNSON, Texas	MICHAEL R. McNULTY, New York
JENNIFER DUNN, Washington	WILLIAM J. JEFFERSON, Louisiana
MAC COLLINS, Georgia	JOHN S. TANNER, Tennessee
ROB PORTMAN, Ohio	XAVIER BECERRA, California
PHILIP S. ENGLISH, Pennsylvania	KAREN L. THURMAN, Florida
JOHN ENSIGN, Nevada	
JON CHRISTENSEN, Nebraska	
WES WATKINS, Oklahoma	
J.D. HAYWORTH, Arizona	
JERRY WELLER, Illinois	
KENNY HULSHOF, Missouri	

A.L. SINGLETON, *Chief of Staff*

JANICE MAYS, *Minority Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT

NANCY L. JOHNSON, Connecticut, *Chairman*

ROB PORTMAN, Ohio	WILLIAM J. COYNE, Pennsylvania
JIM RAMSTAD, Minnesota	GERALD D. KLECZKA, Wisconsin
JENNIFER DUNN, Washington	MICHAEL R. McNULTY, New York
PHILIP S. ENGLISH, Pennsylvania	JOHN S. TANNER, Tennessee
WES WATKINS, Oklahoma	KAREN L. THURMAN, Florida
JERRY WELLER, Illinois	
KENNY HULSHOF, Missouri	

LETTER OF TRANSMITTAL

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON OVERSIGHT,
Washington, DC, August 6, 1998.

Hon. BILL ARCHER,
*Chairman, Committee on Ways and Means,
House of Representatives, Washington, DC.*

DEAR CHAIRMAN ARCHER: The purpose of this letter is to transmit to the full Committee on Ways and Means the report of the Subcommittee on Oversight on the year 2000 problem, commonly known as "Y2K," as it relates to the major program areas within the Committee's jurisdiction. This report was approved by the Subcommittee on August 6, 1998.

The United States, with almost half the world's computer capacity and 60 percent of the world's Internet assets, is the most advanced, and most dependent, producer and user of information and telecommunications technologies. Most computers, computer systems, and telecommunications networks in use in the Federal Government today will not be able to function in the year 2000 and beyond unless they are modified.

This is of particular concern as it applies to the Federal programs within the jurisdiction of the Committee on Ways and Means, including those administered by the U.S. Department of the Treasury, U.S. Department of Health and Human Services (HHS), and the Social Security Administration (SSA). Among the major programs are tax and trade administration, Medicare, and Social Security. The computers serving the programs within the Committee's jurisdiction affect more than 260 million Americans. The revenue programs affect every taxpayer and every business, and the benefit programs impact the health and well-being of millions. These Americans rely on the vital services they receive and cannot afford to have them disrupted by computer failures; nor can they afford to have the computers produce erroneous penalty assessments, notices, refund or benefit checks.

Most of the computers in use in the Federal Government today store information for a year in a two-digit format. While fixing the two-digit year format is technically simple, the process for analyzing, renovating, and testing computers and computer systems, including embedded computer chips, to identify and correct the errors involves a very complex management task. A massive logistical effort is also needed for those computers and systems that must interact, including those that interact through telecommunications networks. Telecommunications networks are critical to Social Secu-

rity checks getting to seniors, hospitals and doctors being paid by Medicare, and taxpayers being properly and efficiently served by the Internal Revenue Service (IRS). For these services to continue into the year 2000 without disruption, each of these agencies must successfully renovate their own systems and be able to effectively interact with the renovated systems of the Treasury Department's Financial Management Services (FMS), which has responsibility for actually making the payments to the beneficiaries and taxpayers.

Further complicating this technical, managerial, and logistical challenge is the fact that most of the systems that the agencies must renovate are old and have software written in nearly obsolete programming languages. Agencies have encountered serious problems in their earlier attempts to modernize these antiquated systems, especially in delivering systems that provide the required functionality on schedule and within budget.

Modifying computer code requires programming skills that are in short supply. Recruiting and retaining qualified personnel is a major concern, which will undoubtedly become more difficult and expensive as the year 2000 draws closer.

In response to your request, the Subcommittee on Oversight held two hearings on the Y2K problem to identify the issues that need to be effectively addressed for the major programs within the Committee's jurisdiction to continue to provide critical services without disruption in the year 2000 and beyond. The Subcommittee hearings focused on the implications of the Y2K computer problem for program beneficiaries and taxpayers, potential risks to program missions, and major remaining program vulnerabilities.

On May 7, 1998, the Subcommittee on Oversight held its first Y2K hearing. Federal program officials testified on the progress they have made in renovation efforts, the risks they have identified, and how they are attempting to mitigate those risks. Representatives of major financial services institutions, including those who interact with the agencies that administer these programs, testified along with information system industry observers on their Y2K experience, the most perplexing Y2K challenges remaining, and actions needed to prevent disruptions in program services. On June 16, 1998, the Subcommittee held its second hearing on Y2K issues as they relate to telecommunications. The Subcommittee received testimony from representatives of various segments of the telecommunications industry and other industry observers, who described relevant Y2K issues, progress toward addressing those issues, and the remaining challenges. The Subcommittee also received testimony and related study reports from the U.S. General Accounting Office (GAO) in both of its Y2K hearings.

Issues raised at the Subcommittee's Y2K hearings included the importance of making Y2K conversion a national priority; the adverse impact potential legal liability is having on Y2K information sharing and communications; and the adequacy of funding and other resources available for the required system renovations. Many of these Y2K issues have been the subject of other Congressional oversight hearings, dating as early as April 1996, which have encouraged the administration to establish Y2K as a national priority and to focus attention on Y2K renovation. On February 4, 1998, President Clinton established the Council on Year 2000 Con-

version. On July 14, 1998, the President presented his first major policy address on Y2K.

With regard to legal liability issues, the administration has taken two initiatives to promote greater Y2K information sharing and communication. The Department of Justice Antitrust Division approved a proposal to allow the discussion and exchange of information on the Y2K issue. This Justice position was intended to ease concerns about information sharing resulting in antitrust action. The other initiative relates to proposed legislation to provide protection against legal liability for those who share in good faith information about Y2K experiences and solutions. However, more needs to be done by the administration as well as the Congress to further these initiatives and resolve the related issues.

Based on its review, the Subcommittee found that SSA is relatively well positioned to have its systems renovated to function properly in the year 2000. This is primarily because SSA was the first to start its Y2K conversion efforts and its management has provided strong and consistent leadership on each phase of the conversion effort. SSA is currently working with FMS to test its entire process, including payments to beneficiaries.

The Subcommittee believes that HHS is in the weakest position, relative to SSA and Treasury, in having its systems renovated in time for the year 2000. The progress of the Health Care Financing Administration (HCFA) is of greatest concern because HCFA, as well as the contractors upon which it relies heavily to process Medicare claims and payments, initially expected to do their processing on a system which has since been abandoned because of major system development difficulties. Therefore, multiple older systems must be renovated by both HCFA and its contractors, and the time remaining to complete the renovations is extremely tight. Other HHS Y2K concerns involve inadequate information about biomedical device readiness, and the late start in renovating systems for welfare and child support programs, which involve numerous interdependencies between State and Federal systems.

Treasury is apparently in a stronger position than HHS, but not as strong as SSA. The major concern is the inadequate progress made to date by the FMS, which provides for the payments for SSA, Medicare, and other Federal programs. IRS is also of concern because of the sheer magnitude of the effort required, the poor record IRS has for modernizing its systems and managing its information systems environment and the status of telecommunications capabilities whose renovation is being done by contractors and managed by the Treasury. The U.S. Customs Service (Customs) has brought new management attention to Y2K to help overcome earlier struggles with systems development projects and a late start in its Y2K conversion efforts.

The assessments made by the Subcommittee on Oversight about the Y2K readiness of the SSA, HHS and Treasury agencies responsible for the major programs within the Committee's jurisdiction are consistent with those made by the Government Management, Information, and Technology Subcommittee (Horn Subcommittee), and by the Office of Management and Budget (OMB).

Based on these assessments, the Subcommittee on Oversight is concerned that, with the possible exception of Social Security, vital

services to taxpayers and beneficiaries may be disrupted or otherwise jeopardized by computer system or telecommunication network failures unless the following recommendations are adopted:

1. The administration should more aggressively promote the Y2K problem as a national priority;
2. Businesses, computer industry suppliers, and others should have the capability to communicate and share information about Y2K problems and solutions without fear of legal liability;
3. Agencies should test their renovated systems fully and ensure they interact with other systems as needed to carry out their related functions;
4. Agencies should develop contingency plans to ensure vital services are not disrupted, since realistically all systems will not be renovated fully by January 1, 2000;
5. Agencies should monitor their Y2K efforts closely to ensure their human resources and expertise are commensurate with the renovation tasks that remain to be completed;
6. The administration and Congress should ensure that Y2K funding is adequate for government agencies to have the resources and expertise needed to update and renovate their systems;
7. Small businesses should be encouraged to take the necessary actions to ensure their computer and telecommunications systems will be able to function properly in the year 2000 and beyond; and
8. The Congress should work with the administration to ensure the necessary oversight is provided so that the Y2K challenge is met successfully.

The Committee may want to consider tax incentives for small businesses to encourage them to proceed expeditiously with needed Y2K renovations. Representative Karen Thurman, a Member of the Subcommittee, has introduced legislation, H.R. 4134, to increase by \$20,000 the amount a small business is permitted to expense for the purpose of making its systems Y2K compliant.

The Subcommittee will continue to be diligent in its oversight activities to ensure vital services to beneficiaries and taxpayers are not disrupted because of Y2K-related system failures or malfunctions. The Oversight Subcommittee has requested that GAO continue its studies of SSA, HCFA, IRS, FMS, Customs, and others. The Subcommittee is also monitoring the efforts of the appropriate Inspector General offices, which have considerable efforts underway to assess system readiness along with validating the renovations reported by the various agencies. The Subcommittee also is coordinating its efforts with the ongoing efforts of the Horn Subcommittee, House Y2K Task Force, Senate Special Committee Year 2000 Technology Problem, OMB and the Council on Year 2000 Conversion to monitor the Federal agencies' and private sector progress and readiness for the year 2000.

We hope our assessments and recommendations will provide useful guidance to the Committee in addressing this critical challenge.
Sincerely,

NANCY L. JOHNSON
Chairman
WILLIAM J. COYNE
Ranking Member
ROB PORTMAN
JERRY KLECZKA
JIM RAMSTAD
JOHN S. TANNER
JENNIFER DUNN
KAREN L. THURMAN
PHILIP S. ENGLISH
WES WATKINS
JERRY WELLER
KENNY HULSHOF

Attachments

CONTENTS

	Page
Letter of Transmittal	iii
Background	1
Subcommittee Hearings	2
Other Congressional Oversight of the Y2K Problem	4
Administration Action on the Y2K Challenge	4
Information-Sharing Initiatives	4
Assessment of Y2K Readiness for the Major Programs Within the Jurisdiction of the Committee on Ways and Means	5
Oversight Subcommittee Recommendations	6
Appendix I: Ways and Means Subcommittee on Oversight Hearing on Year 2000 Issues Relative to Programs Within Its Jurisdiction, May 7, 1998	9
Purpose	9
Witnesses	9
Hearing Synopsis	10
Remaining Challenges—Agencies' Perspectives	10
Magnitude of the Challenge—Independent Perspective	11
A National Mandate	12
Liability Protection	13
Biomedical Devices	13
Telecommunications	13
Appendix II: Ways and Means Oversight Subcommittee Hearing on Year 2000 Telecommunications Issues Relative to Programs Within Its Jurisdic- tion, June 16, 1998	16
Purpose	16
Witnesses	16
Hearing Synopsis	16
Remaining Challenges	17

REPORT OF THE SUBCOMMITTEE ON OVERSIGHT ON THE YEAR 2000 COMPUTER PROBLEM

Background

With tremendous advances in technology in recent decades, governments and businesses worldwide have become increasingly reliant on computers. Telecommunications systems and networks are also critical to the operations of nearly every public and private sector organization. The United States, with almost half the world's computer capacity and 60 percent of the world's Internet assets, is the most advanced, and most dependent, producer and user of information and telecommunications technologies.

Historically, most computers, computer systems, telecommunications networks, and embedded computer chips only store a two-digit number for the year, which makes the year 2000 indistinguishable from the year 1900. Those that are dependent upon this two-digit year format will likely either shut down completely or produce incorrect data. Without proper renovation or replacement, malfunctions will cause many costly problems for both government and commerce. Some computers cannot be modified and must be replaced. Although most of the attention concerning the year 2000 problem, commonly known as "Y2K," initially focused on computers and computer systems, there is a growing recognition of the vulnerabilities of telecommunications networks, because a single noncompliant component could potentially shut down an entire network. In addition, there are many items, like elevators and security systems, that are not generally thought of as computer systems but have embedded computer chips. Many of these embedded chips are date-dependent and require replacement in order to function properly in the year 2000 and beyond.

Most computers, computer systems, telecommunications networks, and embedded chips in use in the Federal Government today will not be able to function in the year 2000 and beyond unless they are modified. This is of particular concern as it applies to the Federal programs within the jurisdiction of the Committee on Ways and Means, including those administered by the U.S. Department of the Treasury, U.S. Department of Health and Human Services (HHS), and the Social Security Administration (SSA). Among the major programs are tax and trade administration, Medicare, and Social Security. The computers serving the programs within the Committee's jurisdiction affect more than 260 million Americans. The revenue programs affect every taxpayer and every business, and the benefit programs impact the health and well being of millions. These Americans rely on the vital services they receive and cannot afford to have them disrupted by computer failures; nor can they afford to have the computers produce erroneous penalty assessments, notices, refund or benefit checks.

While fixing the two-digit year format is technically simple, the process for analyzing, renovating, and testing computers and computer systems to identify and correct the errors involves a very complex management task. A massive logistical effort is also needed for those computers and systems that must interact, including those that interact through telecommunications networks. Telecommunications capabilities are critical to Social Security checks getting to seniors, hospitals and doctors being paid by Medicare, and taxpayers being properly and efficiently served by the Internal Revenue Service (IRS). For these services to continue into the year 2000 without disruption, each of these agencies must successfully renovate their own systems and be able to effectively interact with the renovated systems of the Treasury Department's Financial Management Services (FMS), which has responsibility for actually making the payments to the beneficiaries and taxpayers.

Most of the systems that the agencies must renovate are old, further complicating this technical, managerial, and logistical challenge. Agencies have encountered serious problems in their earlier attempts to modernize the antiquated systems, especially in delivering systems that provide the required functionality on schedule and within budget. For example, IRS and Health Care Financing Administration (HCFA) have had difficulty renovating or replacing their old systems and have had to abandon previous modernization plans. Some systems are too old to renovate and need to be replaced, which requires considerable time and expertise. The software has often been written in nearly obsolete languages, and the computer code has been changed numerous times over the years without adequate documentation.

Modifying this computer code requires programming skills that are in short supply and may not be readily available. Modifying telecommunications components and networks requires unique expertise that has also been in short supply. Some agency officials expressed concern over their ability to recruit and retain information systems employees with the necessary expertise to handle the conversions, and even their ability to supplement their work force with contractor support, because of the escalating demand for a finite talent pool and the escalating costs for that expertise. Costs are not the only issue, as specialized knowledge of agencies' sometimes antiquated systems is not easily transferable, if at all, to other employees or contractors. In the recently enacted IRS restructuring bill, Congress provided the IRS Commissioner with personnel flexibilities that will allow him to attract the technical and managerial skills needed to handle such challenges as Y2K.

Subcommittee Hearings

On May 7, 1998, the Subcommittee on Oversight held a hearing to explore Y2K issues for the programs within the jurisdiction of the Committee on Ways and Means (See Appendix I). The Subcommittee explored the management plans and processes the relevant agencies had initiated to renovate or replace their systems. Of particular interest to Subcommittee Members were the implications of the Y2K problem for various program beneficiaries, potential risks to program missions, and major remaining program vulnerabilities. Agency officials, private sector representatives, and

U.S. General Accounting Office (GAO) witnesses testified on the risks and mitigation strategies related to Y2K problems.

The private sector witnesses, in particular, called for the President and Congressional leaders to establish the Y2K problem as a national priority, and to ensure the problem gets the attention, funding, and other resources necessary for success. Among the issues of great concern identified by the witnesses at the hearing for agency attention were: priority setting, progress monitoring, system testing, contingency or continuity planning, and resource and expertise availability. Telecommunications capabilities were also of concern because of the agencies' increasing reliance on outside suppliers and carriers for renovated components and networks, as well as the lack of information as to how those renovations were proceeding. Of particular concern was how the renovation efforts of private sector telecommunications suppliers and carriers correspond to Federal Government agency timeframes for renovating, testing, and implementing their computer systems, as well as for devising their contingency plans.

On June 16, 1998, the Subcommittee held a hearing on the nation's telecommunications infrastructure (See Appendix II). The infrastructure is composed of the public sector network (hundreds of local telephone companies and long distance carriers), the Internet, and millions of government and private sector telecommunications and computer networks. The Subcommittee studied the impact that the Y2K problem may have on the telecommunications infrastructure, and how major programs within the Committee's jurisdiction may be affected. Specifically, the Subcommittee explored implications of critical infrastructure component failures on tax administration, Medicare, Social Security, and other programs within the Committee's jurisdiction. A Federal Communications Commission official, telecommunications industry observers and representatives, and a GAO witness testified on the Y2K readiness of the industry, and the remaining risks and challenges.

For example, witnesses said that testing posed unique risks for telecommunications renovations, because the entire infrastructure cannot be taken out of production to validate the renovated components in their normal operating environment. Nevertheless, they also said that testing telecommunications components and networks to the extent possible is crucial to successful renovations, and establishing contingency plans in the event of telecommunications failures or malfunctions are important to ensure that operations are not at risk.

Another difficult issue raised was the reluctance of telecommunications firms to share information about the readiness of their components or networks because of fear about vulnerability to liability lawsuits. As a result, agency officials did not know whether renovated telecommunications components would be delivered to them in time for testing. The officials recognized that they needed to test their entire system and network configuration to ensure their programs would run properly in year 2000 and beyond. This dilemma, however, is not unique to telecommunications firms, as electric power companies and others have also expressed concern about their vulnerabilities to liability, and have therefore been reluctant to share Y2K-related information.

Other Congressional Oversight of the Y2K Problem

Congress has recognized Y2K as a problem with serious implications for the government, commerce, and the economy. The Subcommittee on Government Management, Information, and Technology, of the Committee on Government Reform and Oversight, held the first of a series of Y2K hearings on April 16, 1996. That Subcommittee has been joined in many of its oversight hearings by the Subcommittee on Technology, Committee on Science. A House Y2K Task Force has also been appointed to provide Congressional leadership on this problem, which complements the efforts of the Senate's Special Committee on Year 2000 Technology Problem. Many other committees have been active in their oversight of the Y2K problem as it relates to programs within their jurisdictions. Congressional oversight has encouraged the administration to make Y2K a higher priority and give it the focused attention needed to ensure systems are renovated properly in time to prevent vital services from being discontinued and disruptions to government, commerce, or the economy.

Administration Action on the Y2K Challenge

The President's budget for Fiscal Year 1999 included about \$2.25 billion for Y2K renovations and related contingencies. On February 4, 1998, President Clinton established the Council on Year 2000 Conversion and named John Koskinen to be its Chairman and Assistant to the President on Y2K matters.

On July 14, 1998, the President presented his first major policy address on Y2K. The President stressed the urgency of the challenge. He lauded the efforts underway by people in the Congress, government, and business—especially those of John Koskinen. He asked Congress to fully fund his budget. The President specifically pointed out that too many businesses, especially small and medium sized firms, will not be ready unless they begin to act now.

He issued three challenges to the business community. First, he called for every business to take responsibility for making sure it is ready by assessing its exposure, asking its vendors and suppliers to be ready as well, and developing contingency plans in case critical systems fail or vendors fail to deliver. Second, he said businesses should exchange and pool information among themselves in order to learn from one another's experiences and solutions. Third, businesses should inform customers about what is being done to address the Y2K problem to help maintain confidence. The President described two initiatives to encourage more open communication on Y2K experiences and solutions: (1) a Department of Justice position relative to antitrust, and (2) proposed legislation to limit legal liability. These initiatives are discussed further below.

Information-Sharing Initiatives

The Antitrust Division of the Department of Justice (Justice) presented its position on the exchange of information about resolving the Y2K computer problem in a July 1, 1998, approval of a private sector information-sharing proposal from the Securities Industry Association to let its members and their computer services suppliers discuss and exchange information on the Y2K issue. Justice

stated that sharing information about the Y2K problem would not lessen competition in the procurement of computer services. Justice also stated that the information sharing would not pose competitive risks unless it involved the disclosure of pricing or customer information. Justice further said that the information exchanges should not diminish competition among the Association's members and might even have a procompetitive effect by reducing costs and/or speeding up the resolution of Y2K issues.

The administration sent proposed "Good Samaritan" legislation to the Congress on July 27, 1998, entitled the "Year 2000 Information Disclosure Act". The proposal would establish a uniform standard of legal liability to protect those who share Y2K information in good faith from claims based on disclosures and exchanges of information. This narrow protection from liability would extend only to the good faith sharing of information and would not provide protection from liability should systems not work properly in the year 2000 and beyond.

Representative David Dreier and Representative Christopher Cox introduced H.R. 4140 on July 16, 1998, which is legislation to (1) limit the financial liability of companies that take steps to avoid Y2K failures, and (2) provide a targeted antitrust exemption to encourage corporate cooperation in solving problems. This proposed legislation would effectively codify the Justice antitrust position, and provide broader liability protection than the "Good Samaritan" legislation.

Assessment of Y2K Readiness for the Major Programs Within the Jurisdiction of the Committee on Ways and Means

Based on its review, the Subcommittee determined that SSA is relatively well positioned to have its systems renovated to be able to function properly in the year 2000. The Subcommittee was impressed with SSA's early planning and conscientious management. This is primarily because SSA was the first to start its Y2K conversion efforts and its management has provided strong and consistent leadership on each phase of the conversion effort. Additionally, SSA has already renovated a large portion of its systems and is proceeding with systems testing and continuity planning.

The Subcommittee believes that HHS is in the weakest position, relative to SSA and Treasury, to have its systems renovated in time for the year 2000. The progress of HCFA is of greatest concern. HCFA, as well as the contractors upon whom it relies heavily to process Medicare claims and payments, initially expected to be using a new Medical Transaction System. That system, however, was abandoned because of major system development difficulties. Multiple older systems must now be renovated by both HCFA and its contractors, and the time needed to complete the renovations is a major concern. HCFA management is also concerned about its ability to compel its contractors to maintain the capability necessary to continue Medicare processing. Consequently, the administration has proposed legislation to reform HCFA's relationship with its contractors. The contractors, on the other hand, suggest that they only need funding and guidance from HCFA to renovate their systems in time. HCFA has also raised concerns about its ability to do the renovations along with the programming changes needed

to implement the Balanced Budget Act and other new provisions which it claims may place a strain on both the time and resources available. Other HHS Y2K concerns involve inadequate information about biomedical device readiness, and the late start in renovating systems for welfare and child support programs.

The Subcommittee assessed Treasury as being in a stronger position than HHS, but not as strong as SSA. Some of its major program areas have not yet demonstrated sufficient progress, even though management attention to Y2K has significantly improved. The major concern is inadequate progress made to date by FMS, which provides for the payments for SSA, Medicare, IRS and other Federal programs. FMS has recently changed management and has recognized the need to be more focused on its Y2K readiness. The IRS is also of concern because of the sheer magnitude of the effort required to update its systems, and the poor track record IRS has for modernizing its systems and managing its information systems environment. Commissioner Charles O. Rossotti has personally made this a priority. Among the Commissioner's top concerns are telecommunications systems which are being renovated by contractors and managed by Treasury. The U.S. Customs Service (Customs) has brought new management attention to Y2K to help overcome earlier struggles with systems development projects and a late start on its Y2K conversion efforts.

The assessments made by the Oversight Subcommittee about the Y2K readiness of the agencies responsible for the major programs within the Committee's jurisdiction are consistent with those made by the Government Management, Information, and Technology Subcommittee (Horn Subcommittee), and by the Office of Management and Budget (OMB). The Oversight Subcommittee based its assessments primarily on its two Y2K hearings and related research. Based on quarterly reports from all the federal departments on Y2K status and progress, as well as on other information about Y2K renovation efforts, the Horn Subcommittee has graded each department's Y2K performance, and OMB has ranked departments by tiers.

Oversight Subcommittee Recommendations

The Subcommittee is concerned that, with the possible exception of Social Security, vital services that programs within the Committee's jurisdiction provide to taxpayers and beneficiaries may be disrupted or otherwise jeopardized unless the following recommendations are adopted:

1. The administration should more aggressively promote the Y2K problem as a national priority;

The President has established the National Council on Year 2000 Conversion, presented a major policy address, and proposed legislation to limit liability. It is equally important the administration use the many resources at its disposal to elevate the profile of this critical issue and energize the public through the press and in public events.

2. Businesses, computer industry suppliers, and others should have the capability to communicate and share information about Y2K problems and solutions without fear of legal liability;

Proposed legislation intended to encourage information sharing on Y2K experiences and solutions needs to be passed in order to allow focus of the private sector on solving Y2K problems rather than being concerned about vulnerability to lawsuits for the information they may share. This information sharing should benefit not only those currently trying to renovate their systems, but also those who have not yet begun the renovation effort by allowing them to take advantage of the experience of others.

3. Agencies should test their renovated systems fully and ensure they interact with other systems as needed to carry out their related functions;

Testing is critical to identifying renovation problems before systems are put into use and to prevent beneficiaries or taxpayers from being adversely affected. Those with testing experience have cautioned that fully testing a system may take about three times longer than initially expected, and as much as half the total time needed for an entire system renovation. System or end-to-end testing is particularly important to successful renovation, especially for determining the ability to interact with others upon whom one must rely on to carry out the mission. This testing is particularly difficult for the telecommunications systems. Consequently, renovations must be done in a timely manner, no later than the March 31, 1999, date set by the Office of Management and Budget, to be able to identify and effectively correct problems. The necessary resources, expertise, and techniques also need to be secured in time to be applied properly.

4. Agencies should develop contingency plans to ensure vital services are not disrupted, since realistically all systems will not be renovated fully by January 1, 2000;

Contingency or continuity plans are critical for all systems, even those thought to be renovated, because there may be disruptions or failures in power, water, or telecommunications that may not be within the control of an agency. There must be sufficient time and resources provided for these plans, including time and resources to test their validity and effective implementation. This issue will become more critical as 2000 draws closer and it becomes more evident which systems may not be renovated in time. This planning must also be done to ensure the best options are considered for maintaining the continuity of vital program services.

5. Agencies should monitor their Y2K efforts closely to ensure their human resources and expertise are commensurate with the renovation tasks that remain to be completed;

The IRS Commissioner and others raised concerns about the resources available to renovate old systems and to reprogram obsolete computer code. The agencies received some additional assistance when the administration provided authority for the agencies to recruit retirees with needed expertise to supplement the current work force. As the demand for information systems and telecommunications expertise increases, it may be necessary to find other innovative ways to secure the needed talent.

6. The administration and Congress should ensure that Y2K funding is adequate for government agencies to have the resources and expertise needed to update and renovate their systems;

Witnesses at the Subcommittee's hearings suggested that the funding requested by the administration may not be sufficient to complete renovations, which may become apparent as agencies proceed with their efforts. The certainty of the funding will be necessary to allow agencies to make comprehensive Y2K plans and secure the needed resource and expertise, including contractor support. The adequacy of funding and resources needs to be monitored closely as the scarcity of the requisite expertise may cause Y2K costs to escalate as time becomes a greater factor.

7. Small businesses should be encouraged to take the necessary actions to ensure their computer and telecommunications systems will be able to function properly in the year 2000 and beyond; and

Small businesses may be the most vulnerable to Y2K system failures because many have not yet started Y2K renovations and may not have the resources, expertise, or funds to do the necessary renovations. With the importance of small business to the vitality of the nation's economy, the Committee may want to consider tax incentives for small businesses to encourage them to proceed expeditiously with needed Y2K renovations. Representative Karen Thurman, a Member of the Subcommittee, has introduced legislation, H.R. 4134, to increase by \$20,000 the amount a small business is permitted to expense for the purpose of making its systems Y2K compliant.

8. The Congress should work with the administration to ensure the necessary oversight is provided so that the Y2K challenge is met successfully.

The Congress must maintain vigilant oversight of the Y2K efforts. The emphasis of congressional oversight to date has been on systems status and renovation progress. The emphasis will likely need to shift to what will not be renovated in time, and what can be done to ensure the continuity of services. Oversight should also be properly targeted to maintain the focus of those responsible for the renovation on getting the job done right.

The Subcommittee intends to continue to be diligent in its oversight activities to ensure vital services to beneficiaries and taxpayers are not disrupted because of Y2K-related system failures or malfunctions. The Oversight Subcommittee has requested GAO to continue its studies of SSA, HCFA, IRS, FMS, Customs, and others. The Subcommittee will also monitor the efforts of the appropriate Inspector General offices which have considerable efforts underway to assess system readiness, along with validating the renovations reported by the various agencies. The Subcommittee also is coordinating its efforts with the ongoing efforts of the Horn Subcommittee, House Y2K Task Force, Senate Special Committee Year 2000 Technology Problem, OMB and the Council on Year 2000 Conversion to monitor the Federal agencies' and private sector progress and readiness for the year 2000.

APPENDIX I

WAYS AND MEANS SUBCOMMITTEE ON OVERSIGHT
HEARING ON YEAR 2000 ISSUES RELATIVE TO PRO-
GRAMS WITHIN ITS JURISDICTION, May 7, 1998**Purpose**

The hearing explored the year 2000 issues for the major program areas within the jurisdiction of the Committee on Ways and Means. In particular, the Subcommittee examined the implications of the year 2000 computer problem, commonly known as "Y2K," for the various program beneficiaries, the potential risks to program missions, and major remaining program vulnerabilities.

Witnesses

Agencies—

The Honorable Charles O. Rossotti, Commissioner, Internal Revenue Service

The Honorable John Callahan, Assistant Secretary, Office of Management and Budget, U.S. Department of Health and Human Services

Mr. John Dyer, Principal Deputy Commissioner, Social Security Administration

Mr. James A. Flyzik, Assistant Secretary, Information Systems and Chief Information Officer, U.S. Department of the Treasury

Ms. Constance E. Craig, Assistant Commissioner, Information Resources, Financial Management Services, U.S. Department of the Treasury

Ms. Vincette Goerl, Assistant Commissioner, Finance, U.S. Customs Service, U.S. Department of the Treasury

Private Sector—

Mr. John Bace, Research Director, Gartner Group, Inc., Rosemont, Illinois

Mr. Harris N. Miller, President, Information Technology Association of America

Mr. Steven McManus, Communications Manager, BankBoston, Boston, Massachusetts

Ms. Irene Dec, Vice President, Information Systems, Prudential Insurance Company of America

Ms. Jennifer Jackson, General Counsel, Connecticut Hospital Association, on behalf of American Hospital Association

Ms. Mary Nell Lehnhardt, Senior Vice President, Office of Policy and Representation, Blue Cross and Blue Shield Association

U.S. General Accounting Office—

Ms. Lynda D. Willis, Director, Tax Policy and Administration Issues, General Government Division; accompanied by Ms. Sherrie Russ, Assistant Director

Mr. Joel C. Willemsen, Director, Information Resource Management, Accounting and Information Management Division; accompanied by Mr. Randy Hite, Assistant Director

HEARING SYNOPSIS

The private sector witnesses admonished the Subcommittee to do whatever it can to make solving the Y2K problem a national priority. The Subcommittee was reminded that the United States has close to half the world's computer capacity and 60 percent of Internet assets, making the U.S. the world's most advanced and dependent user of information technology. The Subcommittee was also cautioned that if these systems many of which perform functions and services critical to the nation suffer disruption, it could create a widespread crisis.

The agency officials testified on the progress that they have made in their conversion efforts, the risks they have identified, and how they are attempting to mitigate those risks. The officials described Y2K as their number one technology priority with each expressing a keen awareness of the importance of successfully meeting this challenge. They described the extensive resources that they have committed to ensure an orderly computer conversion. They also articulated the considerable risks that they still face, and the efforts that they are undertaking to manage those risks and thereby avert potentially catastrophic implications for Social Security and Medicare beneficiaries and taxpayers. While each voiced confidence that their agencies were on schedule to meet this considerable challenge, they recognized the enormity of the task ahead, and the reliance they must place in others for their own success.

Remaining Challenges—Agencies' Perspectives

IRS Commissioner Charles Rossotti, a highly successful technology professional, acknowledged that he is still learning about the magnitude of this effort, as it presents the largest conversion and testing challenge known to him. His counterparts agreed with his assessment, with everyone expressing the belief that they were doing everything within their power to meet the challenge. For the most part, the agencies' officials testified that they are currently performing the computer conversions identified as being needed, with some having tested the converted systems. The tasks remaining include completing system conversion and testing, performing integrated or end-to-end tests of entire processes, independently validating successful conversion, and developing contingency plans should system disruptions arise. Some of these tasks involve working with other organizations with which an agency shares data or upon which it relies to carry out its processes. For example, IRS and SSA share important account information and both rely on FMS to produce checks for taxpayers or beneficiaries, respectively. Some agency officials expressed concern over their ability to retain information systems employees with the necessary expertise to handle the conversions, and even their ability to supplement their work force with contractor support, because of the escalating demand for a finite talent pool and the escalating costs for that expertise. Costs are not the only issue, as specialized knowledge of agencies' sometimes antiquated systems is not easily transferable, if at all, to other employees or contractors. At the time, this issue was not expressed as a critical impediment, but it remains a concern as the year 2000 approaches.

Magnitude of the Challenge—Independent Perspective

Neither the private sector panel nor the GAO witnesses questioned the determination or accounts of the agency officials to ensure they meet this substantial challenge, but they did raise concerns about how much remains to be done and how little time there is to do it. The private sector witnesses stressed the magnitude of the challenge as being immense, much greater than they had initially thought. They said their efforts began over three years ago, which is fortuitous because the conversion and testing has taken every bit of that time and more. For example, a private sector witness said that testing had taken three times longer than expected and 50 percent of the entire conversion time for her organization.

A GAO witness cited a recently issued report entitled YEAR 2000 COMPUTING CRISIS: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships. This report credits agencies with the progress they have made, but concludes that with the remaining risks and current pace not all mission-critical systems will be successfully converted in time. GAO calls for more action to mitigate the remaining risks to avoid debilitating results. GAO also cites vulnerabilities in vital economic sectors of the nation, like telecommunications, health, safety, and small business. Interdependencies of related systems across public and private sectors increase the risk of a cascading wave of failures or interruptions of essential services. The report also discusses similar interdependencies of related systems internationally.

GAO acknowledged that as the year 2000 has drawn nearer and the scope of the challenge has become clearer, the Federal Government's response to the crisis has grown as well. GAO credited Congressional oversight as being key to increasing the focus of OMB and agency attention on the Y2K problem. For example, after numerous Congressional oversight hearings on the need for more focused Y2K attention, in February 1998, the President issued an executive order establishing a President's Council on Year 2000 Conversion to recognize the national and international aspects of the problem.

John Koskinen, who was named the Assistant to the President and Chair of the Council, differed with GAO on the leadership role the Council should play in implementing numerous GAO recommendations. However, in his formal response to the GAO report, he agreed that issues involving the economic sectors, along with others that are national or international, are beyond the control of individual Federal agencies. He believed that his role needs to be as a catalyst, facilitator, and coordinator, and that the Council should only create and directly manage new national forums for specific sectors of the economy, such as energy and telecommunications. Mr. Koskinen has, in fact, created such national forums and has taken a global approach to his new duties. The Subcommittee agrees with GAO and Mr. Koskinen that the last thing needed at this time is the creation of a new bureaucracy. However, Mr. Koskinen does not have the authority to compel partnerships between public and private sectors; among economic sectors; or across local, State, Federal, and other countries' governments.

A National Mandate

Chairman Johnson asked GAO to give thought to how to formulate a national mandate to make sure that people responsible for system renovations get the needed information and action in time to mitigate any risks and avert a disaster. GAO discussed the following findings in its recently issued report:

Setting priorities is critical. As it becomes increasingly evident that there is not enough time to successfully convert all mission-critical systems across the Federal Government, it is imperative that the Executive Branch identify those systems, that if not fixed, could most seriously threaten health, safety, national security, or economic well-being. These priority systems must also be able to interact with data or processes that are shared. Contingency plans should be developed immediately for those systems not deemed to be high priority to ensure sufficient time and resources are available.

Monitoring agencies' progress must be comprehensive and reliable. The reports on agency progress must include all agencies and systems, including those sharing information, and include data that accurately reflects their status relative to the expectations for each phase of conversion and time remaining available for conversion.

Testing, including end-to-end testing, for entire processes must be performed. Sufficient time, resources, and expertise must be made available to do this critical testing so problems can be identified and corrected before the system is in production. This is an area in which agencies have generally not been as diligent as necessary. Most agencies have said they want to use all or most of 1999 for this end-to-end testing, although some schedule slippage may affect their ability to do so.

Requiring independent verification and validation of Y2K programs, including testing, is critical to the integrity of the conversion process. Agencies may use Inspector Generals' Offices, contractors, and others with the requisite expertise to ensure their Y2K program has the necessary steps to ensure each phase is completed, thoroughly and accurately. This must be done independently of officials with conversion responsibility.

Developing contingency or business continuity plans is imperative. Such plans must be developed for all systems to ensure that the processes or programs served will be able to function in the event successful conversion is not completed on time. The plans may require functions to be handled through manual processes, other converted systems, or other means for working around nonconverted systems. The plans must also consider any interdependencies with other systems.

Developing a resource strategy is essential. OMB and OPM have already taken some actions to help agencies to attract and retain personnel with the requisite expertise to carry out the conversions, but agencies need to identify creative ways to ensure they have the necessary resources beyond the year 2000. Likewise, similar plans must be developed and actively monitored to ensure the funds, personnel, other expertise, and equipment are available when needed.

Establishing an ability to address governmentwide issues needs strengthening. Numerous issues are beyond the control of any particular agency, such as responsibility or control over various economic sectors or governments. These issues may need to be addressed by a broader authority to make the necessary arrangements for agencies to ensure their systems are, in fact, fully and successfully converted.

Liability Protection

Chairman Johnson asked both the private sector and GAO panelists how to avoid Y2K problems. The liability protection issue was identified by several witnesses as the crux of industries' reluctance to share information or deliver Y2K certified equipment or components. It was raised specifically about biomedical devices or equipment and telecommunications components.

Biomedical Devices

The American Hospital Association witness offered some suggestions for Congress in her written statement, including the following idea on liability protection:

Congress should enact some form of immunity from liability for health care providers that have taken steps to prevent year 2000 problems from affecting patient care for example, relying on the FDA's data base of medical devices and equipment for information about year 2000 compliance . . . Providers should not be liable for damages for the year 2000 limitations of those products and systems.

The HHS testimony discussed the initiative HHS has taken with over 16,000 biomedical equipment manufacturers, which has resulted in a FDA Internet web site of manufacturers' information about the Y2K compliance of their equipment. A GAO witness told the Subcommittee that GAO is looking into the biomedical device area, including the FDA web site, for another committee. He offered a preliminary observation that manufacturers' information is just now coming forward and has sometimes changed from initial postings.

Telecommunications

Both the IRS Commissioner and Treasury Chief Information Officer expressed concern about telecommunications, with their concern centered around vendor schedules for delivering releases of their components or systems that are certified as Y2K compliant. Treasury bureaus cannot plan on testing the telecommunications aspects of their systems until vendor delivery is made, nor can they proceed with end-to-end testing. Both GAO witnesses cited telecommunications as a major concern for all agencies since they have to rely on vendors to deliver compliant components or systems. The reason this concern rises above others is that the telecommunications industry has not been very forthcoming with information about exactly when and what it will be able to deliver and certify as Y2K compliant. The industry is thought to be quite concerned about its liability exposure and has chosen not to put out information until it is absolutely certain of its validity. The later information and deliveries are, the greater the difficulty for agencies with regard to component or end-to-end testing as well as contingency

planning. Realistically, with the normal procurement cycle times needed, agencies cannot pursue alternative suppliers especially since nearly the entire industry is in the same position. With an increasing reliance on telecommunications for providing services to beneficiaries and taxpayers, and so much still unknown about compliant deliveries, telecommunications is a serious and widespread vulnerability for agencies' Y2K programs.

Since the hearing, the Subcommittee staff has further explored with GAO the validity of the industry's belief that protection is needed against liability and the posture agencies find themselves on this issue. The GAO officials illustrated the frustration shared across agencies by describing a meeting of industry representatives and agency officials, that was arranged by the CIO Council, to better understand one another's needs. Not all of the key vendors attended, with some last minute cancellations, and little information was exchanged even on the reasons for the industry's reluctance to be more forthcoming. So, the Subcommittee is left with a concern that the industry is more worried about liability than in the agencies' needs for specific information.¹

At a briefing for Congressional staff on May 22, 1998, John Koskinen said he has Assistant Attorney General Joel Klein's agreement that the Department of Justice Antitrust Division to write a business advisory to let companies know that sharing information across industries to facilitate Y2K compliance will not be viewed as an antitrust violation. [The business advisory was issued on July 1, 1998.] Mr. Koskinen said the other reason for vendor reluctance to share information is, in his opinion, bad legal advice. He believes sharing information on compliance efforts actually protects vendors against legal liability, and he offers that observation to any audience that he addresses.

As discussed above relative to IRS, the Subcommittee understands that the telecommunications sector is concerned about liabilities that may arise from Y2K failures and is reluctant to share information about the capabilities of its systems or components until they are tested and delivered. There may very well be other reasons for telecommunications companies reluctance to share information, for example, they may not have compliant components yet or are concerned about the compliance of their components in different agency environments. Regardless, this reluctance to share information presents a dilemma for agencies that cannot be certain when they will get delivery and be able to test in their own environment, including end-to-end testing.

Some agencies, including IRS, have recently taken a more aggressive posture with their telecommunications vendors to promote better communications. IRS, Treasury, and TRW have recently formed teams to work together to install and test Y2K components or systems in test facilities, with plans to have the teams pursue testing in the IRS processing environment. SSA has also worked

¹The same basic concerns about increasingly restrictive information flow between industry and government agencies were raised for the electric utility industry in a recent hearing held by Chairwoman Constance Morella before the Science Subcommittee on Technology, Committee on Science. The concerns were raised by agency officials and trade association representatives about having to be reliant on the electric utilities delivery of Y2K compliant equipment, including upgrades to imbedded chips, with little specific information on what will be delivered, when, and at what cost.

with its vendors to obtain specifics on delivery schedules, and related costs, as well as to reduce those specifics to contractual commitments. GSA officials advised the Subcommittee that they are seeing some recent progress in information availability from vendors about the compliance of their components, but vendors are still reluctant to put out information until the components have been successfully tested. Apparently not much of the related software development has been completed. While there are some reports of a recent increase in information flow, that flow must be continued and expanded.

This communication may help ease some anxiety, but reliance on the industry to deliver compliant components in time to be properly tested is a concern as the Y2K deadline approaches. Many deliveries are expected this fall, with any slippage likely to cause constraints in testing plans which pose risks to the affected agencies. Another risk as time passes is whether the vendors will be able to produce enough of the Y2K compliant components, including embedded chips, to satisfy all of their customers' needs. Therefore, the agencies must have firm contractual arrangements in place as soon as possible to set delivery quantities, times, and costs. Should they have reason to doubt the vendors can deliver as specified, the agencies should provide for contingency arrangements secondary suppliers, system workarounds, or other ways to ensure their missions can be accomplished.

APPENDIX II

WAYS AND MEANS OVERSIGHT SUBCOMMITTEE HEARING ON YEAR 2000 TELECOMMUNICATIONS ISSUES RELATIVE TO PROGRAMS WITHIN ITS JURISDICTION, June 16, 1998

Purpose

The hearing explored the Y2K issues for the nation's telecommunications infrastructure and its impact on the major programs within the jurisdiction of the Committee on Ways and Means. In particular, the Subcommittee examined the implications of the Y2K risks posed by the telecommunications infrastructure, including those posed by critical infrastructure component failures.

Witnesses

Agencies—

The Honorable Michael Powell, Defense Commissioner, Federal Communications Commission; and Chairman, Telecommunications Subcommittee, President's Commission on Year 2000 Conversion

Private Sector—

Mr. David Baker, Managing Director, Schwab Washington Research Group

Mr. Gerald A. Roth, Vice President, Technology Programs, GTE Labs Technology and Systems, Alexandria, Virginia

Mr. John Pasqua, Director, AT&T, Warren, New Jersey

Ms. Ronnie Lee Bennett, Vice President, Program Management, Lucent Technologies, San Ramone, California

Ms. Pricilla Gutherie, Vice President and General Manager, TRW, Fairfax, Virginia

Mr. William O. White, Senior Director, Information Technologies, U.S. West, Denver, Colorado

U.S. General Accounting Office—

Mr. Joel Willemsen, Director, Information Resources Management, Accounting and Information Management Division

HEARING SYNOPSIS

During the Subcommittee's Y2K hearing on June 16, 1998, the witnesses described recent progress that has been made in making various facets of the telecommunications infrastructure Y2K compliant, as well as initiatives to improve information sharing and communications about Y2K compliance within the telecommunications industry and its customers. The witnesses, however, also described concerns about their vulnerability to legal liability and other impediments to more open communication. They also talked about the remaining challenges to making the telecommunications infrastructure Y2K compliant, including the fact that even after extensive testing of components and networks, the compliance of the entire infrastructure cannot be verified until the year 2000 because it cannot be taken down to test in its entirety. Therefore, effective contingency planning is particularly important for those who rely heavily on telecommunications for carrying out their missions.

These issues relate to the state of Y2K readiness for the telecommunications industry in the United States, which is thought to be much further advanced than its counterparts overseas.

Collectively, the witnesses described the telecommunications infrastructure as being a complex web of components including switches, routers, systems, and networks that operate together to transmit voice and data. The infrastructure provides a seamless interconnectivity between a wide range of networks and carriers. Telecommunications has become critical to the operations of nearly every public and private sector organization. The witnesses described the process being used to ensure that each part of the infrastructure will be able to operate properly in the year 2000 and beyond. The process is essentially the same as the one used for ensuring Y2K compliance for computer systems; that is, awareness, assessment, renovation, validation, and implementation. They described the industry as generally being through the assessment phase and well into renovation, with compliant components expected to be ready for customer delivery by the third or fourth quarter of 1998. These components, for the most part, will have been laboratory tested when delivered and will need only to be tested in the organization's production environment.

The witnesses said that each phase of the process must be completed to ensure the compliance of each component, and must be carefully coordinated to ensure the desired interoperability of the entire telecommunications infrastructure. They singled out testing of the infrastructure as unique because it cannot realistically be replicated or taken out of operation to be tested. Therefore, while components may be certified as Y2K compliant, there is no real assurance that they will be compatible or function properly in operation on January 1, 2000. Consequently, contingency plans are particularly important for organizations to have alternate ways to carry out their missions in the event of failure in their telecommunications capability.

Remaining Challenges

The Subcommittee learned that the telecommunications industry is generally well aware of the magnitude of the Y2K problem and is proceeding to renovate and test components for delivery to customers in the third or fourth quarter of 1998. The industry is probably further along in its renovations than the agencies within the Committee's jurisdiction expect it to be according to their testimony in the Subcommittee's May 7, 1998, hearing. The industry representatives explained that there has been a reluctance to share information about Y2K readiness of components because of the fear that the information could be used against a supplier or carrier in a liability lawsuit. As a result, telecommunications firms have been reluctant to make information available, even to customers, until they have tested renovated components, rather than take the chance that they would have to modify information upon learning more about a component's compliance. Even though the firms know that more information would be helpful for their customers to manage their own Y2K renovation programs, many in the industry remain so concerned about being subjected to a lawsuit that they are reluctant to share more information.

Some industry witnesses suggested that Congress could ease this reluctance to share information by passing legislation to provide limited protection against lawsuit for those who share information in good faith to help reduce Y2K-related problems. They said there was a separate effort underway with the Department of Justice Antitrust Division for industry to get some assurance from Justice that sharing information for the purpose of solving the Y2K problem would not be considered as an anticompetitive practice or violation of the antitrust laws. [On July 1, 1998, Justice formally established this position in response to a request from the Security Industry Association.] While such a Justice position should ease concerns about information sharing on Y2K subjecting an organization to antitrust suit by the government, the industry witnesses said that legislation would be needed to provide some protection against private lawsuit.

While the concern about legal liability continues to have a dampening effect on information sharing, the witnesses described a number of efforts and forums that are being used within the telecommunications industry to improve the flow of information about the readiness of various components. One industry observer offered that among the reasons for information lagging on telecommunications was that everyone was initially focused on their own internal computer systems. Now that they realize they are also dependent on others, like telecommunications carriers and suppliers, more attention is being afforded those interdependencies. Both agency and industry witnesses testified that many in the telecommunications industry have been aware of the Y2K issue and working on it for years, as early as 1995. They acknowledge more information is being made available as testing forums have emerged, but also advocate the need for liability protection. The AT&T witness challenged others to join its recent initiative to put information out for public and customer consumption, while agreeing that relief would be welcome.

The TRW witness provided the perspective of a systems integrator, and articulated the dilemma the constrained information flow poses for customers of telecommunications components. She said among the most important things to do is effectively scheduling the renovation, testing, and implementation of components; and among the most difficult is reacting to suppliers and carriers who do not deliver compliant components consistent with that schedule. While the agency witnesses at the Subcommittee's May 7 hearing expressed frustration with not knowing when their telecommunications vendors were going to be able to deliver, the industry witnesses at this hearing said, for the most part, they will be delivering Y2K compliant components to their customers in the third or fourth quarters of 1998 after they have been tested in Bellcore or other labs. They also said that they are now communicating their schedules with their customers. The Lucent witness said the company expected to be able to satisfy all of its customers' orders for components, but also urged others who have not yet determined their needs to do so as quickly as possible so their needs can be considered in Lucent's production schedules.

While testing is a critical issue for Y2K readiness for all organizations, the telecommunications aspects of testing are unique in a

couple of ways. Telecommunications components may test as Y2K compliant when tested individually or even in a test lab, but may not function properly in a customer's production environment. Interoperability testing is an important aspect of the testing regime which to some extent can be done in a lab, but must also be done in the production environment. However, even with this testing, there cannot be complete assurance that the entire telecommunications infrastructure is Y2K compliant until it is in operation on January 1, 2000. This, as the witnesses explained, was because the infrastructure cannot realistically be taken down to test its compliance. The industry is working through cooperative arrangements to test components both individually and as they may normally be configured in operations. It is also working with customers to design interoperability testing in the customer's operating environment to mitigate as many of the risks as they can. These tests, however, will not be done before year-end 1998 in most organizations because the telecommunications components will not be delivered in time to do them earlier.

The limitations of interoperability testing for the telecommunications infrastructure makes contingency planning essential as well as difficult since organizations are becoming increasingly reliant on telecommunications to carry out their missions. The witnesses were uniform in their belief that organizations must be prepared for the possibility that they may have some telecommunications outages, and make provisions for getting their work done during those outages. While considerable time remains to develop such contingency plans, those plans will require resources, logistics, and other considerations that must be provided for well in advance of the ultimate need. The Federal Communications Commission witness said the FCC intends to continue to encourage the industry to proceed expeditiously to make the infrastructure Y2K compliant to minimize the likelihood of failure. His concerns were far more pronounced for international compliance since he does not believe the same amount of awareness and attention have been given to Y2K as has been by the domestic telecommunications industry. For that reason, he is chairing the Year 2000 Conversion Council Telecommunications Subcommittee, and believes those organizations reliant on telecommunications for conducting international business must be particularly diligent in providing for effective contingencies. The GAO witness agreed with the importance of contingency planning in this area and offered a guide his office has published to assist those in devising effective plans.

