# EXECUTIVE SUMMARY

The Committee has found that the most frustrating aspect of addressing the Year 2000 (Y2K) problem is sorting fact from fiction. Reports from even the most reputable news sources fall prey to polarizing forces—either over emphasizing a handful of Y2K survivalists, or downplaying the event as a hoax designed to sell information technology equipment.

The Internet surges with rumors of massive Y2K test failures that turn out to be gross misstatements, while image-sensitive corporations downplay real Y2K problems. The good news is that talk of the death of civilization, to borrow from Mark Twain, has been greatly exaggerated. The bad news is that Committee research has concluded that the Y2K problem is very real and that Y2K risk management efforts must be increased to avert serious disruptions.

Y2K is about more than the failure of an individual's personal computer or an incorrect date in a spreadsheet. As one examines the multiple layers of systems and technologies that support our everyday lives, the potential Y2K problems increase exponentially. The interdependent nature of technology systems makes the severity of possible disruptions difficult to predict. Adding to the confusion, there are still very few overall Y2K technology compliance assessments of infrastructure or industry sectors. Consequently, the fundamental questions of risk and personal preparedness cannot be answered at this time.

On the positive side, Y2K awareness is growing. In the past year, both public and private institutions have doubled their efforts to find, evaluate, and address Y2K risk exposure. The Committee has seen a significant amount of progress since its inception. However, Senate hearings, interviews, and research have not produced convincing evidence that the Y2K problem is well in hand.

The biggest Y2K impact may occur internationally. While the U.S. should have started its Y2K preparations earlier, worldwide preparations generally lag even further behind.

## OVERALL OBSERVATIONS

**Many organizations critical to Americans' safety and well-being are still not fully engaged in finding a solution.**

For example, over 90% of doctors' offices and 50% of small- and medium-sized businesses have yet to address the problem. Larger firms have, in general, grasped how a Y2K failure could severely impact their businesses and are taking steps to remedy the problem. Smaller firms remain more focused on what they perceive as more immediate concerns, which in many cases do not include Y2K.

**Most affected industries and organizations started Y2K remediation too late.**

As a result, many organizations must exercise "triage"—focusing on what is critical to sustain the life of the enterprise as opposed to finding long-term solutions.

**Self-reporting has yielded unreliable assessments for most industry sectors. With few exceptions, disclosure of Y2K compliance is poor.**

Analogous to letting students grade their own tests, self-reporting offers data of varying reliability. Nonetheless, it has become the standard in both private industry and government. Industry surveys are currently the most widely utilized tool to measure compliance. Unfortunately, the results of many surveys have been kept from public and Special Committee view (see "Transportation" in this report). Despite an SEC rule requiring Y2K disclosure of public corporations, companies are reluctant to report poor compliance levels.

**Fear of litigation and loss of competitive advantage are the most commonly cited reasons for bare-bones disclosure.**

Although sharing Y2K data could save time in companies' remediation and contingency planning efforts, such cooperation has not been forthcoming. To encourage greater disclosure, the Committee spearheaded a bipartisan effort that passed the Year 2000 Information Readiness and Disclosure Act (S.2392) and introduced the CRASH Protection Act (S.1518). The Year 2000 Information Readiness and Disclosure Act provided a basic level of protection for Y2K statements made in good faith. The CRASH Protection Act pressured the SEC to require more meaningful Y2K corporate disclosure to shareholders.

More legislation may be necessary to address Y2K litigation. Some liability cost projections are as high as $1 trillion. Serious doubts exist as to whether or not the present judicial system could handle a potentially monstrous wave of litigation.

The Committee plans to address certain key sectors in 1999 where there has been extreme reluctance to disclose Y2K compliance.

**National emergency and security planning for Y2K-related systems failures is just beginning.**

FEMA contingency plans are in draft form, but there is no national, strategic plan to assure that critical infrastructures will continue to function.

This is partially due to varying levels of state and local government preparedness. State and local governments represent the first line of defense in emergency situations, and emergency planning is difficult without their full involvement. A recent Labor Department report stated that several states are lagging in specific Y2K system repairs relating to federally funded programs.

**Leadership at the highest levels is lacking.**

A misconception pervades corporate boardrooms that Y2K is strictly a technical problem that does not warrant executive attention. Some government sectors lack clear directives and policies on Y2K.

## SECTOR ASSESSMENTS

Since its establishment in April 1998, the Special Committee has held nine hearings on seven critical economic sectors:

- Utilities
- Health care
- Telecommunications
- Transportation
- Financial institutions
- Government
- General business

The eighth sector, Litigation, will be addressed in early 1999.

The Committee plans to revisit each of the sectors in 1999, with emphasis on litigation and the addition of international concerns to the list of critical sectors. The Committee will assess the nation's progress toward Y2K compliance and pinpoint problem areas. The Committee will also continue to provide recommendations to Congress for legislative action.

## UTILITIES

**While some compliance efforts are behind, the utility industry as a whole is configured to handle interruptions, blackouts, and natural disasters. A prolonged, nationwide blackout is not likely to occur. However, local and regional outages remain a distinct possibility depending upon the overall preparedness of the individual electric utility serving a given area.**

The nation's electric power industry comprises 3,200 independent utilities. Overall remediation of the electric power industry is slow. According to NERC, only about 50% of the utilities had completed Y2K remediation as of December 1998. Failure of some parts of the electric industry's system is likely, but the Committee does not expect the integrity of the overall power grid to be compromised. Of greatest concern are approximately 1,000 small, rural electric utilities that may not have the resources to devote to Y2K compliance.

Compliance among oil and natural gas utilities is also progressing slowly. A survey by the Committee, while limited in scope, indicates a lack of contingency planning, overly optimistic assertions that compliance will be complete, and a lack of knowledge about suppliers' Y2K status.

## HEALTH CARE

**The health care industry lags significantly in its Y2K preparations compared to other sectors. Because of limited resources and lack of awareness, rural and inner-city hospitals have particularly**

**high Y2K risk exposure.**

Health care is the nation's single largest industry, generating $1.5 trillion annually. There are 6,000 hospitals, 800,000 doctors and 50,000 nursing homes, as well as hundreds of biomedical equipment manufacturers and suppliers of blood, drugs, linens and bandages—and health care insurers—that may be unprepared for the year 2000.

According to a report by the Gartner Group, 64% of hospitals—primarily smaller hospitals—have no plans to test their Y2K remediation efforts. In addition, 90% of physicians' offices are unaware of their Y2K exposure. Struggling compliance efforts by HCFA (the agency that oversees Medicare) and unaddressed concerns about medical devices are major roadblocks to the industry's Y2K readiness.

## TELECOMMUNICATIONS

**A massive industry-wide effort is underway to assess the impact of Y2K on telecommunications. The initial interoperability testing indicates that the U.S. communications will transition without significant problems. Currently, more than 80% of public network systems have been tested and are considered compliant.**

The telecommunications industry has spent billions on Y2K fixes and should have 99% of access lines in compliance by the fall 1999. Currently, industry and government are working together to coordinate contingency plans in case there are failures. Industry in U.S. and overseas has established warning networks to alert each other of Y2K problems.

## TRANSPORTATION

**The transportation sector is the linchpin for just-in-time inventory management across most every sector, from health care supplies to food. The Y2K readiness of this sector is critical to our global economy. Planes will not fall out of the sky, but disruption of flights and global trade between some areas and countries may occur.**

On average, the nation's 670 domestic airports started Y2K compliance too late. The Federal Aviation Agency has made great strides in the past year, but remains at risk. The situation with international air traffic control and airports is much more severe. The maritime shipping industry has not moved aggressively toward compliance. Public transit could be seriously disrupted.

## FINANCE

**ATMs are expected to function correctly and banks should have adequate cash to meet consumer demand, based on a Federal Reserve estimate that each American household will withdraw an average of $500. The securities industry has responded well to its internal Y2K issues and has undertaken expansive testing. However, fund managers and brokers have only recently started to consider the implication of corporate Y2K vulnerability on investment decisions.**

The financial services sector ranks ahead of nearly all other industries in its remediation and testing efforts. Legislation in Congress and action by the Committee have led to legal requirements on broker-dealers and publicly traded companies to disclose compliance information.

Federal regulators have made considerable progress in tracking compliance among banks, thrifts and credit unions, of which 95% have received satisfactory government ratings.

## GOVERNMENT

**Several state and many local governments lag in Y2K remediation, raising the risk of service disruption. The federal government will spend in excess of $7.5 billion and will not be able to renovate, test, and implement all of its mission critical systems in time. However, wholesale failure of federal government services is not likely to occur.**

The Committee's work in this sector includes national emergency planning as well as federal, state, and local government preparedness. After a late start, FEMA is now engaged in national emergency planning in the event of major and minor Y2K disruptions.

State and local governments vary widely in their Y2K preparations. Several states are not prepared to deliver critical services such as benefit payments. Of greatest concern to the Committee is the ability of local communities to provide 911 and emergency services.

The federal government also varies widely in its Y2K preparations. The Social Security Administration started early and is prepared, while other agencies, like the Department of Defense, are lagging. To its credit, the federal government publicly displays its Y2K status through quarterly and monthly reports to the Office of Management and Budget.

## GENERAL BUSINESS

**In general, large companies have dealt well with the Y2K problem, due to greater resources. Very small businesses may survive using manual processes until Y2K problems are remediated. However, many small- and medium-sized businesses are extremely unprepared for Y2K disruptions. One survey shows that more than 40% of 14 million small businesses do not plan to take any action.**

The heavily regulated insurance, investment services, and banking industries are furthest ahead in their efforts: health care, oil, education, agriculture, farming, food processing, and the construction industries are lagging behind. The cost to regain lost operational capability for any mission critical failure will range from $20,000 to $3.5 million, with an average of 3 to 15 days necessary to regain lost functions.

## LITIGATION

The prospect of litigation arising from Y2K-related failures has shadowed the Committee's work from the very beginning. Some estimates project litigation cost in excess of $1 tril-

lion. The Committee plans to hold hearings and work closely with the Judiciary and Commerce Committees to make legislative proposals in this area.

## INTERNATIONAL

**Several U.S. trading partners are severely behind in their Y2K remediation efforts. For example, the Gartner Group estimates that Venezuela and Saudi Arabia (two of the largest U.S. oil importers) are 12 to 18 months behind the U.S. in their Y2K remediation efforts.**

The Committee is greatly concerned about the international Y2K picture. The U.S. is dependent on a healthy global economy. It is in the interest of the U.S. to encourage Y2K remediation worldwide.

* * * * *

The challenges posed by the Y2K problem are numerous and daunting. The Special Committee conducted extensive research and held numerous hearings in 1998, but still cannot conclusively determine how extensive the Y2K disruptions will be. The Committee has no data to suggest that the United States will experience nation-wide social or economic collapse, but the Committee believes that some disruptions will occur, and that in some cases Y2K disruptions may be significant. The international situation may be even more tumultuous.

There are reasonable steps individuals may take to prepare for the Year 2000. Consumers are urged to keep copies of financial statements and ask local banks what efforts are being made toward Y2K compliance. Individuals should research companies' compliance levels before making investment decisions. The Y2K problem has been likened to a winter storm, with the implication that similar preparation is appropriate. Americans should prepare for Y2K based on facts and reasonable predictions about the problem's effects on vital services.