Group, Chase Manhattan and J.P. Morgan. These six institutions have collectively estimated their Y2K costs to be over $2.4 billion. Additionally, the estimated cost of Y2K repairs is increasing, as shown in figure 2.

Figure 2. Y2K Repair Estimates[6]

Company	*Past Est. (millions)*	*New Est. (millions)*
Aetna	$139	$195
ATT	$300	$900
Bankers Trust	$180-$230	$220-$260
Cendant	$25	$53
Chase Manhatt.	$300	$363
General Motors	$400-$500	$890
McDonald’s	$8	$30
Merrill Lynch	$375	$560
Sears	$63	$143
Xerox	$116	$135

Can’t we develop an easy Y2K fix?

Popular sentiment suggests that a technological quick fix will appear just in time to kill the millennium bug. So far, “quick fix” claims have proved to be claims for a particular product that may show promise in one particular application, for example, finding where the actual dates and date processing routines are hidden in a program.

Software programs and computer hardware vary too greatly to be fixed by one solution. Currently, there are over 500 programming languages in use. A universal or broadly applicable Y2K solution would have to be compatible with many or most of these languages. Additionally, finding all the dates and date processing in an estimated 36,000,000 programs[7] is an enormous task difficult to automate.

The embedded processors pose another problem. Although the percentage of embedded chips with a Y2K problem is estimated to be relatively small, potentially millions of chips exist that may have to be replaced. Unfortunately, most of them are not readily accessible or easily modified.

Where can I learn more about the Y2K problem?

Many solid references can be found in the endnotes of this section and elsewhere in this report. An enormous amount of Y2K information resides on the Internet. However, legitimate information is buried among overstated rumors and half-truths. As with most other information derived from Internet sources, Y2K information must be verified for accuracy.

Additional information can be obtained through the Committee’s website at www.senate.gov/~y2k and the President’s Council on Year 2000 Conversion’s website at www.y2k.gov.

CRITICAL INFRASTRUCTURES

Critical infrastructures can include both computerized services and physical services essential to minimum functioning of economy and government. More than abstract systems, critical infrastructures enable the average person to use an

ATM, make a phone call and fly on an airline. In the past, many of these key infrastructures or sectors were separate. However, advances in information technology have caused many of these systems to be interconnected and linked through networks. The Committee has approached the critical infrastructures by examining the Y2K work occurring both vertically within specific sectors and horizontally across different interrelated sectors, such as banking and telecommunications.

Recognizing that the Y2K problem could have serious implications on the smooth functioning of our defense and economy, Senator Moynihan wrote President Clinton in July of 1996 and suggested a special Y2K commission. While Senator Moynihan's suggestion was not taken, Executive Order 13010 created the President's Commission on Critical Infrastructure Protection. The Commission was not tasked to study Y2K, but it recognized the potential for the Y2K problem to cause long-term problems in the infrastructures. Due to late starts, many organizations have contracted out work on sensitive systems. In some cases, organizations are sending code overseas to foreign firms. The correction of code overseas could lead to increased incidents of corporate espionage and intentional cyber disruptions. The broad scope of Y2K corrections could allow an adversary to build an exceptional understanding of sensitive systems thus enabling it to "design a subtle or comprehensive attack" against critical systems.[8]

THE QUESTION IS NOT WILL THERE BE DISRUPTIONS, BUT HOW SEVERE THE DISRUPTIONS WILL BE.
-SENATOR DODD

It is absolutely vital that the owners, operators and regulators of the nation's critical systems continue to be aware that Y2K may provide an opportunity for those with malicious intent. Sandia National Laboratories warned the Committee that:

"Thinking that we will be so preoccupied with Y2K that we would not notice deliberate malicious intent, terrorists, hackers and other criminals might see Y2K as a prime opportunity to attack pieces of our infrastructure. Or they might use Y2K-induced infrastructure failures as cover for theft, arson, bombings, etc. We must be watchful of such groups in the months leading up to Y2K and we must be especially careful when monitoring the crisis as it occurs to discern deliberate intent." [9]

Current national security and emergency preparedness policies are not designed for the challenges of the information age. The U.S. needs a system or process whereby the government can coordinate responses with the privately owned and operated critical infrastructures. We must build the broad based contingency plans necessary to ensure that the national security and emergency preparedness posture of the U.S. is not compromised by Y2K. The U.S. must remain ready to mitigate the (economic, emergency or security) effects that could be caused by Y2K.

Y2K is an opportunity to educate ourselves first hand about the nature of 21st century threats. Technology has provided the U.S. with many advantages, but it also creates many new vulnerabilities. Recognizing shifts in the technological topography of the nation requires vision. Reverting to a world without microchips or technology-dependent systems is not only undesirable, but also impossible. Instead, we, as a nation and as individuals, need to consider carefully our reliance on information technology and the consequences of interconnectivity, and work to protect that which we have so long taken for granted.

FORMATION OF THE SPECIAL COMMITTEE

Senator Robert Bennett first identified the Year 2000 as an issue for the legislative agenda in 1996 as the Senate organized for the 105th Congress. He shared his concerns with Senator Alfonse D'Amato, Chairman of the Senate Banking Committee, who urged Senator Bennett to take up the issue in his new role as Chairman of the Subcommittee on Financial Services and Technology.

The Subcommittee naturally focused its first efforts on the regulators' efforts to ensure Y2K compliance. In February 1997 and again in April 1997, Senators D'Amato and Bennett requested information on Y2K preparations from the following financial regulatory agencies:

- The Federal Reserve Board (FRB)
- The Federal Deposit Insurance Corporation (FDIC)
- The Office of Thrift Supervision (OTS)
- The National Credit Union Administration (NCUA)
- The Office of the Comptroller of the Currency (OCC)
- The Securities and Exchange Commission (SEC)

Shortly after the Committee inquiry, the Federal Financial Institutions Examination Council (FFIEC), an inter agency body made up of FRB, FDIC, OTS, NCUA and OCC, issued guidelines for the financial institutions and federal examiners to focus on issues they must address to avoid major service disruptions due to Y2K.[10]

Individual agency responses revealed varying degrees of readiness. The SEC's response detailed extensive plans for remediation and testing, while other agencies demonstrated little more than a general awareness and initial response to the problem. Many of the regulatory agencies deferred to statements published by FFIEC without providing any substantive information about their own progress. These results prompted Senator Bennett to conduct the first hearing on financial services and the Year 2000 on July 10, 1997.