

1999

## Aviation and the Year 2000: What's the Big Deal

April F. Robbins

---

### Recommended Citation

April F. Robbins, *Aviation and the Year 2000: What's the Big Deal*, 64 J. AIR L. & COM. 835 (1999)  
<https://scholar.smu.edu/jalc/vol64/iss3/9>

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Journal of Air Law and Commerce by an authorized administrator of SMU Scholar. For more information, please visit <http://digitalrepository.smu.edu>.

## AVIATION AND THE YEAR 2000: WHAT'S THE BIG DEAL?

APRIL F. ROBBINS

### PREFACE TO REPORT ON AVIATION AND THE YEAR 2000

**S**INCE THE DATE this article was completed in October of 1998, substantial progress has been made, and reported, concerning aviation-related Y2K remediation. This includes reports concerning the progress of the FAA and other such organizations. Although the reports seem rather glowing, they must be viewed for what they really are, a self-reported examination.

For example, the FAA recently reported that a hundred percent of its mission critical systems, 424 in total, are certified as Y2K compliant.<sup>1</sup> This is based upon the FAA's internal examination of its systems, utilizing its own definitions for "compliance." In fact, the FAA's certification process is currently being reviewed and validated by the Department of Transportation Inspector General and the General Accounting Office. That report has not yet been issued, and as stated before, Y2K "compliance" is a broad, vague concept. It does not necessarily mean that no Y2K-related failures will occur.

Further, the FAA's pronouncement is particularly suspect in light of the June 15, 1999, announcement by Republican representative Steve Horn's Technology Subcommittee. In that announcement, the Technology Subcommittee reported that the Y2K readiness of governmental agencies reveal that only 2 out of 43 "high impact" federal government programs will be ready for the year 2000. Specifically it was reported that:

The Office of Management and Budget (OMB) has identified 43 federal "high impact" programs that provide critical services to millions of Americans nationwide, such as food stamps, Medicare, Child Welfare and the Air Traffic Control System. How-

---

<sup>1</sup> See <http://www.faa2k.com/html/progress.html> (visited July 16, 1999).

ever, Horn's Subcommittee judges that only *two* (Social Security and National Weather Service) of these major impact programs are Y2K compliant. Some of them will not be ready until December 1999.

"Unbelievable. These are the programs that the Administration itself has determined *must* continue to function," said Dick Armyey. "I think everyone agrees that we can't be without programs like the Air Traffic Control System when the Year 2000 dawns."<sup>2</sup>

Y2K concerns are legitimate, and many airlines have determined that they will not fly on January 1st. Reasons given include concerns with air traffic control of various facilities, as well as concerns regarding the availability of insurance. A number of airlines have recently issued statements indicating their decisions to cancel January 1, 2000, flights. On July 13, 1999, Poland's national airline LOT indicated it would ground all its planes on January 1, 2000, "to avoid millennium bug problems, in what is thought to be the first mass cancellation in Europe due to Y2K worries."<sup>3</sup> Vietnam Airlines has canceled its flights, and Qantas Airlines and Indonesia's PT Garuda may do likewise.<sup>4</sup>

... Qantas expressed confidence in its own readiness but admitted that risks lay with airports and air traffic control authorities around the world if computer systems suffer Y2K-related breakdowns.<sup>5</sup>

Domestically, litigation has continued to be an overwhelming concern of many companies, including those in aviation. On July 20, 1999, President Clinton finally signed the Year 2000 Readiness and Responsibility Act into law.<sup>6</sup> This law, approved by the House in an overwhelming vote of 404/24, is designed to limit lawsuits from tying up U.S. court rooms. It is expected that creative plaintiffs' attorneys will attempt to find any holes in the immunities that the Act provides. Nevertheless, the protections set forth in the Act are now available and should limit or eliminate many claims.

In short, the aviation industry, like every other, will likely suffer some repercussions of the infamous Y2K bug. Internal com-

---

<sup>2</sup> See <http://freedom.house.gov/y2k/news/pr990615.asp> (visited July 27, 1999).

<sup>3</sup> See [http://cnnfn.com/1999/07/13/Europe/wires/lot\\_wg/](http://cnnfn.com/1999/07/13/Europe/wires/lot_wg/).

<sup>4</sup> *Id.*; see also [http://cnnfn.com/1999/03/31/worldbiz/airlines\\_bug/](http://cnnfn.com/1999/03/31/worldbiz/airlines_bug/) (visited July 16, 1999).

<sup>5</sup> *Id.*

<sup>6</sup> See <http://hillsource.house.gov/digital/y2k> (visited July 27, 1999).

pliance does not insulate a company, nor an industry. Each entity must assess the risks associated with external vendors and other variables outside the scope of its control. Y2K is a risk-management issue. It should be analyzed as such. That much has not changed since the article was originally drafted.

### TABLE OF CONTENTS

I. HISTORY OF THE PROBLEM .....	838
II. WHERE THE PROBLEMS EXIST .....	840
III. FOREIGN COUNTRIES .....	842
IV. FEDERAL AVIATION ADMINISTRATION .....	844
V. AIRPORTS .....	848
VI. AIRLINES .....	852
VII. AIRCRAFT .....	854
VIII. AIR TRAFFIC MANAGEMENT/NAVIGATION ....	856
IX. TRAVEL RESERVATIONS .....	858
X. INSURANCE .....	858
XI. BUSINESS APPLICATIONS/MAINTENANCE ....	863
XII. REMEDIATION .....	864
XIII. GENERAL ACCOUNTING OFFICE PROCEDURE .....	865
A. AWARENESS .....	865
B. ASSESSMENT .....	866
C. RENOVATION/CONVERSION .....	868
D. TESTING/VALIDATION .....	869
E. IMPLEMENTATION .....	869
XIV. CONTINGENCY PLANS .....	869
XV. CONCLUSION .....	870

January 1, 2000. The date will likely have much more significance than one might think. Once the calendar rolls over to 2000, a programming glitch will affect electronic and computer equipment all over the world. Some equipment may not be affected at all, while some may fail temporarily, and some may be rendered totally obsolete and nonfunctional. This phenomenon is known as the "millennium bug" or Year 2000 ("Y2K"); and it is coming. Because electronics have become so entrenched in our day-to-day routines, Y2K will likely impact everyone in some fashion, especially in the business world. An analysis of Y2K as a business management problem, with a particular emphasis on aviation, has revealed that the problems it will create are common to all fields, but some are unique to aviation. Knowing what the potential problems are, where they

manifest themselves, how they are being addressed, and how they should be addressed will provide some insight into protection, prevention, and planning.

## I. HISTORY OF THE PROBLEM

Most people think that the Y2K issue is a "computer problem." That misconception has arisen because the problem is the result of early technology. In the infancy of computers and technology, programs and data were recorded on Hollerith cards. These data processing cards had to be manually punched with information. This technology consumed substantial time and storage space. To save time and space, a short-cut was adopted to enter dates with only six digits: MM/DD/YY (month/day/year). As technology continued to develop and as computers evolved, this protocol continued in its application. Early computers, although faster than the punch cards, were extremely limited in their capacities and storage space, and available memory was very expensive. One computer could fill an entire room and had minimal capacity, so the practice of using MM/DD/YY continued. Even as technology continued its rapid advancement and memory became less costly, the protocol remained. Foresighted programmers and engineers understood that this short-cut could cause a problem when the year 2000 arrived, but they never anticipated that the equipment and/or the computers employing the technology would still be in operation at that time.

On the surface, the practice of using MM/DD/YY may appear insignificant, but it is not because computers at their most basic level work with numbers. When a computer attempts to manipulate information using the two digits "00," the result can prove fatal to many operations. Most business applications, accounting software, inventory programs, and security systems use only two-digit date fields to specify the year (rather than four digits). When the date "00" is read, many computer programs will prefix "19" in front of the zeros and interpret it as the year 1900 instead of 2000, resulting in various unpredictable responses by the computer. In some business applications, the computer will crash and shut down. Others will try to compute the information using the year 1900, which could provide erroneous results. Potential erroneous responses from business applications include: wrongful calculation of maturity dates on financial instruments, misinterpretation of storage dates for perishable

supplies, improper calculation of time for equipment calibration, and erroneous calendaring and docketing.

Unfortunately, some systems have already issued erroneous information or failed in whole or in part. "The system that Federal Aviation Administration technicians use to track maintenance for radar and navigation equipment has started to spit out false information about when a future check-up is due because it doesn't recognize the year 2000," according to Allyn Dillman of the FAA Electronics Technicians Union.<sup>7</sup> One state's licensing system crashed when faced with processing information on licenses not due to expire until the year 2000 or later.<sup>8</sup> A store's computerized inventory system destroyed tons of corned beef because of a faulty interpretation of the expiration date.<sup>9</sup> A credit card company issued a recall of a number of its credit cards with expirations beyond 1999, and another refused to issue credit cards that had a three year expiration because their equipment could not process those cards.<sup>10</sup> Penitentiary prisoners have been freed prematurely, and the Kansas Board of Education notified a 104 year-old woman to register for kindergarten.<sup>11</sup>

In addition, only one out of every four centesimal years is a leap year. The year 2000 is a leap year, as was 1600, but 1700, 1800, and 1900 were not. Because the year 2000 is a leap year, whereas 1900 was not, if a computer wrongfully interprets "00" to mean 1900, the computer will not recognize the leap year. This may affect those systems that are programmed to operate on a business work schedule. For example, a building may be controlled by an automated thermostat that is programmed to heat/cool the facility during business hours, elevators may only operate on certain schedules, and security systems may be programmed to limit access to buildings during off-peak hours. When a leap day alters the computer's weekly programmed schedule, the building may not be heated or cooled as it should be, access cards may be inoperable, and the elevators may be out of operation.

---

<sup>7</sup> Barbara S. Peterson, *Ghost in the Machine*, CONDE NAST TRAVELER, August 1998, at 31.

<sup>8</sup> See Joel Lanz, *Year 2000 Assessment Process*, in *Understanding, Preventing, and Litigating Year 2000 Issues: What Every Lawyer Needs to Know*, Practising Law Institute June 1998, at 118.

<sup>9</sup> See *id.*

<sup>10</sup> See *id.*

<sup>11</sup> See *id.*

Although many of these problems have already been corrected, they are symptomatic of the type of programming failures that may be caused by the millennium bug. Correcting these computer programs has proven to be a monumental and expensive task.<sup>12</sup>

## II. WHERE THE PROBLEMS EXIST

Because Y2K is the result of a programming anomaly, it may manifest itself in virtually every type of computer application, including accounting programs, word processors, video games, flight simulators, flight planning "avcomps," and the like. With more than four hundred computer languages in operation on thousands of computer systems, time and money are the two primary impediments to remedying the Y2K problem.

Just as it seemed computer specialists were beginning to understand the scope and complexity of correcting computer programs written in hundreds of different languages, using various date calculation codes (some of which are stacked and deeply embedded within programs) another element of surprise surfaced. Not only are computer software programs likely to fail, but any electrical device working with a pre-programmed microchip is likely to experience problems.

Microchips (microprocessors, a.k.a. semiconductor chips or "chips"), approximately the size of a thumbnail, were manufactured utilizing the same six-digit date protocol. Microchips can be found in almost every electronic device. Reportedly, only ten percent of the billions of manufactured chips have been installed in computers.<sup>13</sup> The other ninety percent are installed in such widely used items as answering machines, utility company equipment, manufacturing equipment, microwave ovens, telephones, medical equipment, elevators, drilling rigs, alarm clocks, remote controls, VCRs, vehicles, ATMs, cash registers, credit card machines, gas pumps, traffic lights, railroad switches, navigation systems, satellites, oil derricks, thermostats, security systems, and airplanes. The average person comes into contact with over seventy microprocessors before lunch every day.<sup>14</sup>

---

<sup>12</sup> Office of Governor, *About Time: Managing the Y2K problem in Local Government* (visited August 1999) <<http://www.dir.state.tx.us.y2k.resources/guide2000.htm>>.

<sup>13</sup> Todd Carlson, Former Chief Information Officer for Electronic Data Systems, *The Worldwide Virus: How Not to be Bitten by the Year 2000 Bug*, at the North Texas Commission Panel Discussion (July 16, 1998).

<sup>14</sup> See John L. Peterson, et al., *The Year 2000: Social Chaos or Social Transformation*, (visited April 12, 1999) <<http://www.year2000.com/Y2Karchive.html>>.

Although there are billions of chips manufactured and in operation, it has been estimated that only one to three percent will fail.<sup>15</sup> The questions are, "Which ones?" and "Where are they?" "We spent all this time worrying about codes and not the embedded chips," said Bill Greenwalt, a staff member of the Senate Government Affairs Committee that is looking into the Y2K problem.<sup>16</sup> "Many chips that are being used to perform non-date-sensitive functions actually contain a hidden date calendar that in some cases could cause malfunctions. Most chips are made in bulk and are not custom-designed for just one task," he explained.<sup>17</sup> A company making timers, for instance, will likely decide to "develop a one size fits all chip, or the Mother of All Chips," according to Dr. Mark Frautschi, former Johns Hopkins University physicist.<sup>18</sup> Most likely, he said, "that chip will probably have a date-sensitive area in the background in case some customer needed that function. That date-sensitive area remains on the chip even when it is purchased by customers who have no desire to track dates."<sup>19</sup>

The insidious nature of the Y2K embedded chip problem recently confronted Chrysler Corporation when it shut down its Sterling Heights assembly plant and set all of its plant clocks to December 31, 1999. Although the executives anticipated some computer software problems, the effects were much broader than anticipated. "We got lots of surprises," said Chrysler Chairman Robert Eaton. "Nobody could get out of the plant. The security system absolutely shut down and wouldn't let anybody in or out. And you obviously couldn't have paid people because the time-clock systems didn't work."<sup>20</sup>

This is only one example. One can only imagine how Chrysler's failures would have impacted the organization if the exercise were not experimental. Technological problems cannot be isolated, and a real failure, similar to that described above, without contingencies in place, may have a substantial domino effect because the world and modern business are so interconnected and networked.

---

<sup>15</sup> See Lou Kilzer, *Elusive Millennium Bug Begins Mutating*, *Rocky Mountain News*, July 26, 1998, at 1.

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

<sup>20</sup> Rachael Konrad, *Big 3 Fight 2000 Bug Enforced Upgrade*, *DETROIT FREE PRESS*, April 23, 1998.



Software glitches, embedded chips, and supplier dependency are universal problems for all industries, including aviation. Aviation is likewise dependent upon factories to timely and properly manufacture parts, regulate safety systems, calibrate equipment, and operate test cell facilities. Aircraft assembly plants, Fixed Based Operators (FBOs), and repair facilities are dependent upon just-in-time (JIT) suppliers to deliver parts, accounting firms to pay their invoices and employees, and *all* of these businesses are generally dependent on *outside vendors*.

We have created a world whose efficient functioning in all but the poorest and remotest areas is dependent on computers . . . . And not isolated computers . . . . We have created dense networks of reliance around the globe. We are networked . . . . Whatever happens in one part of the network has an impact on other parts of the network.<sup>21</sup>

These networks reach from the highest level of government to the smallest of businesses, both national and international. Although the United States government and large corporations have already begun to assess their problems, foreign countries and small businesses are not so well prepared. They do not have the funds or manpower to devote to such a daunting task. As a result, they are particularly susceptible to Y2K problems.<sup>22</sup>

### III. FOREIGN COUNTRIES

Literature dealing with international aspects of Y2K indicates that foreign countries are lax in their preparation for Y2K. This has particularly significant ramifications with respect to aviation.<sup>23</sup> An American Airlines representative was reported to have said "I don't think it will be any surprise if we steer clear of a few countries until it is safe. . . ."<sup>24</sup>

There are thirty-two Foreign Flight Information Regions bordering the FAA's National Airspace System.<sup>25</sup> These regions have direct communications with twelve of the FAA's twenty-one

---

<sup>21</sup> Peterson, *supra* note 8.

<sup>22</sup> *Small Business Problems Loom Large, D.C.I.'s IT News Presents Year 2000 Update* (visited Aug. 26, 1998) < <http://year2000.dci.com/article/1998/08/26small.htm>>.

<sup>23</sup> See *Hearing Charter, House Committee on Transportation and Infrastructure Hearing and the Year 2000*, (September 29, 1998) (transcript available at <[http://www.house.gov/science/charter\\_tech\\_09-29.htm](http://www.house.gov/science/charter_tech_09-29.htm)>).

<sup>24</sup> Dominic Rushe & Russel Hotter, *Flights Fear After Millennium Bug: World's Airlines Face Chaos as Computers Threaten Safety*, MAIL ON SUNDAY, Dec. 14, 1997.

<sup>25</sup> See Karl Bremer, *Y2K Are We Ready?*, AIRPORT MAGAZINE, Sept./Oct. 1998.

Flight Information Regions.<sup>26</sup> Additionally, FAA air traffic control systems directly interface with foreign airport approach control and tower facilities in the Pacific, Atlantic, and Caribbean areas.<sup>27</sup> At last count, U.S. air carriers operated in over ninety countries and over more than two hundred foreign airports.

The infamous millennium bug and the ability of developing countries to prepare for it are key concerns at the assembly of the International Civil Aviation Organization (ICAO). Canada's Transportation Minister David Collenette insisted at the ICAO meeting that Canadian airlines and airports will have eradicated the bug in time, but he said he cannot be sure the same will be true in some states in Africa, Latin America, and Asia.<sup>28</sup>

The alarm has sounded, and the world is responding. Many organizations and reporters are very concerned about the failure of foreign countries to meet the Y2K deadline, and the impact it will have on the global economy, including aviation. According to the Deputy Secretary of Transportation, Mortimer Downey, "[t]here are parts of the world where air traffic control is rudimentary and awareness of this issue is almost non-existent."<sup>29</sup> Accordingly, the U.S. might ban its airlines from flying to and from countries that cannot prove that their air traffic control systems are free from Y2K problems.

At the ICAO Annual Meeting, Administrator Garvey warned other nations that she will work with the State Department to recommend that U.S. citizens not fly to countries that have not satisfactorily resolved their Y2K problems.<sup>30</sup> Areas currently causing the greatest concern are Africa, Latin America, and Asia.<sup>31</sup> The International Air Traffic Controllers Union has also cited the Commonwealth of Independent States and other countries that comprise the former Soviet Union as another region where air traffic control problems are already so severe that little attention is being paid to Y2K issues.<sup>32</sup>

Nearly 2,000 airports also need to address the problem, according to the International Air Transport Association (IATA).

---

<sup>26</sup> See *id.*

<sup>27</sup> See *id.*

<sup>28</sup> See *Year 2000 Bug Bothers Airlines*, THE TORONTO STAR, September 23, 1998.

<sup>29</sup> Jennifer Thomas-Bloomberg, *U.S. May Ban Flights to Country not Ready for Y2K*, DOT Says, BUSINESS TODAY.COM, (visited September 11, 1998) <<http://www.businesstoday.com/techpages/y2kban091098.htm>>.

<sup>30</sup> See *Hearing Charter*, *supra* note 17.

<sup>31</sup> See Peterson, *supra* note 1, at 32.

<sup>32</sup> See *Year 2000 Bug Bothers Airlines*, *supra* note 22.

But since every country has sovereignty over its own airspace, there is no guarantee they will. "Ultimately, the airlines will have to make the choice of which country they fly to in the year 2000," says Joe Morgan, head of the International Division of the FAA's year 2000 program. When the date gets nearer, the State Department will gather information from U.S. Embassies and issue bulletins on the readiness of foreign airports—much the way travel warnings are now issued.<sup>33</sup>

To complicate Y2K preparations for foreign countries, January 1, 2000, is the date scheduled for the completion of a conversion to a unified currency for the European community.<sup>34</sup> Concurrently with Y2K remediation, European countries are also facing the extraordinary task of reprogramming their entire financial system to handle a new monetary system, which only complicates the Y2K matter. How Europe will simultaneously address Y2K and successfully transition to a new monetary system presents a unique challenge.

The ICAO, IATA, and similar organizations are actively involved with addressing both international and domestic aviation-related Y2K concerns.<sup>35</sup> There is no doubt that Y2K embodies a host of date-related problems for the aviation industry. The interrelated nature of the problem cannot be isolated to any individual company, and the failure of any one component in the network could immobilize the industry. In this complex network, the most visible component of the industry is the FAA itself.

#### IV. FEDERAL AVIATION ADMINISTRATION

The U.S. has the most heavily computerized National Airspace system. It handles nearly half of the world's air traffic, and its jurisdiction stretches from the Western Atlantic to five hundred miles outside of Tokyo, abutting thirty-two foreign air traffic regions. Not surprisingly, in preparing for the next millennium, the U.S. is expected to spend more than one hundred sixty million dollars on the daunting task of combing through two hundred twenty-two computer programs and some twenty-one million lines of code.<sup>36</sup>

---

<sup>33</sup> See Petersen, *supra* note 1, at 32.

<sup>34</sup> See Capers Jones, *Resource Conflicts Between the Year 2000 and Euro-currency Conversion Problems*, (visited 1997) < <http://www.year2000.com/archive/eurocur.html>>.

<sup>35</sup> See ICAO website devoted to Y2K at <<http://www.icao.int/y2k>>.

<sup>36</sup> See Peterson, *supra* note 1.

Domestically, the readiness of the FAA for the year 2000 is, for the most part, public record. Along with every other governmental agency in the U.S., the FAA is required to report its progress quarterly to the U.S. General Accounting Office (GAO). However, these reports deal *only* with the FAA's remediation of its computer code. The FAA has a very complex and interrelated system of computers.

In 1997, the FAA was required to assess all of its computer equipment and programs and to prioritize and designate those systems that are "mission critical."<sup>37</sup> The criteria considered in making the "mission critical" designation are not fully explained, but the FAA did identify and designate four hundred thirty of its six hundred fifty-five systems as mission critical.<sup>38</sup> Later reports indicate that there may have been a miscalculation of the number of mission critical systems, as reports from the GAO refer to a much smaller number of systems.

To perform its mission, the FAA depends on an extensive array of information processing and communications technologies. Without these specialized systems, the agency cannot effectively control air traffic, target airlines for inspection, or provide up-to-date weather information to pilots and air traffic controllers. For example, each of the FAA's twenty en route air traffic control facilities, which monitor aircraft at the higher altitudes between airports, depend on about fifty interrelated computer systems to safely guide and direct aircraft. The implications of the FAA not meeting the year 2000 deadline are enormous and could affect hundreds of thousands of people through customer inconvenience, increased airline costs, grounded or delayed flights, or degraded levels of safety.<sup>39</sup>

Once designated, the FAA was charged with ascertaining the anticipated operational readiness of those functions to operate in the year 2000. One essential piece of equipment analyzed was the FAA's "critical mainframe computer," a legacy system no longer manufactured by IBM and used by the twenty regional air-traffic control centers for high altitude en route aircraft. The reports concerning the operational readiness of this one piece of equipment vary widely.

---

<sup>37</sup> Honorable Jane F. Garvey, *Federal Aviation Administration Administrator, The Clock is Ticking, Remarks at the International Air Transport Association Annual General Meeting, Montreal, Canada* (June 8, 1998)(transcript available at <<http://www.faa.gov/2k.com/html/remarks.html>>).

<sup>38</sup> *See id.*

<sup>39</sup> *See id.*

On July 22, 1998, the FAA issued a statement that its critical mainframe computer will function properly on January 1, 2000.<sup>40</sup> The conclusion, reached over the past few weeks by programmers, came despite warnings from IBM, the systems manufacturer, that the agency should replace the equipment.<sup>41</sup> According to IBM, "the appropriate skills and tools do not exist to conduct a complete . . . assessment of the . . . computers."<sup>42</sup> Despite the warnings, the FAA hired a number of retired IBM programmers to examine its mainframe. Programmers found that the computers' programs do not utilize the last two digits of the current year when processing dates. Instead, the year is stored as a two-digit number between "01" and "32," assuming that 1975 was year "01." Under that program, the system would calculate the year 2000 as "26". Consequently, the system is not expected to suffer a date-related problem until 2007.<sup>43</sup> The FAA's confidence in the system in light of IBM's warnings is controversial.

As for its other equipment, the FAA reported on July 31, 1998, that sixty-seven percent of its mission critical systems had been renovated.<sup>44</sup> The FAA is replacing forty-four systems, thirty-eight of which are not expected to be in place until June 30, 1999.<sup>45</sup> Once installed, these systems must be evaluated and tested. Given that the FAA will not have these systems in place until June 1999, the FAA's implementation and testing projections appear optimistic. Generally, six to eight weeks are needed to test and implement a single change to an existing system.<sup>46</sup> The FAA has projected that it will have its comprehensive new system tested and implemented in six months, a projection that does not appear realistic.

---

<sup>40</sup> See *Key U.S. Aviation Mainframe Cleared for Y2K*, AIRPORT NET, (Reuters Wired ed.) (visited July 23, 1998) <<http://airportnet.org/depts/regaff/year2k/fun072298.htm>>.

<sup>41</sup> See *id.*

<sup>42</sup> *Air Traffic Control Computer System Cleared for 2000*, WASHINGTON POST, July 22, 1998.

<sup>43</sup> See *id.*

<sup>44</sup> *FAA Systems Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems: Hearings Before The Subcomm. on Technology of The House Comm.*, Pub. No. GAO/T-AIMD-98-251, (visited August 6, 1998) (testimony of Joel C. Willemsen, GAO Director of Civil Agencies Information Systems, Accounting and Information Management Division).

<sup>45</sup> See *id.*

<sup>46</sup> See *id.*

Joel C. Willemsen, Director of Civil Agencies Information Systems for the GAO, presented testimony to the Subcommittee on Technology before the United States House of Representatives that sheds a less-than-optimistic light on the FAA's preparedness.<sup>47</sup> In his testimony, Mr. Willemsen set forth a number of reasons why the FAA is not expected to meet its goal of Y2K compliance. However, he focused mainly on two areas: the year 2000 computer crises and FAA security challenges.<sup>48</sup>

Networking and data exchange problems are serious. Mr. Willemsen's report states:

Though incomplete, FAA's data exchange inventory currently lists 1,386 interfaces, of which 361 exchange date-related data and 341 do not. FAA does not yet know if the remaining 684 interfaces—most of which involve air traffic control systems—exchange date-related data. Of the 361 interfaces that are known to exchange such data, FAA has identified 333 that need repair. Further, FAA does not know how many exchange partners have been contacted, how many agreements have been reached, what these agreements are, or which of them are being implemented.<sup>49</sup>

With respect to external vendors, the FAA must assess the integrity of information received from those entities operating within the airport environment, including airlines, airport authorities, weather reporting agencies, the communications field and other industrial groups, both domestically and internationally.<sup>50</sup> The FAA has not yet identified all of its systems in which date-related information is exchanged with its various outside entities. Assuming that the FAA could meet its ambitious deadline for Y2K compliance, a data exchange with a non-compliant outside source could contaminate the FAA system. Although the integrity of exchange data is a concern, no adequate plan

---

<sup>47</sup> See *id.*

<sup>48</sup> See *id.* (The Y2K topics in this report include: *FAA Reports Progress, but It is Unlikely to Complete Critical Testing Activities in Time*; *FAA Has Not Yet Resolved Cross-cutting Risks That Threaten Aviation Operations*; *Date Exchanges, International Coordination*; *Reliance on the Telecommunications Infrastructure*; *Business Continuity and Contingency Planning*; and finally, *FAA Reports That the Host Computer System Is Renovated, but Testing Is Not Yet Complete.*)

<sup>49</sup> *Id.*

<sup>50</sup> Honorable Jane F. Garvey, *Federal Aviation Administration Administrator, Address to House Committee on Transportation and Infrastructure, the House Committee on Science, Subcommittee on Technology, and the House Committee on Government Reform and Oversight, Subcommittee on Government Management, Information, and Technology*, (September 29, 1998) (transcript available at <[http://www.house.gov/science/garvey\\_09-20.htm](http://www.house.gov/science/garvey_09-20.htm)>) [hereinafter Garvey].

has been devised to protect the FAA from non-compliant incoming data. The FAA has already identified 1,386 data exchange operations.<sup>51</sup>

Finally, in addition to the software and networking concerns facing the FAA, it must also address the embedded chip problem. The FAA faces an overwhelming task of identifying non-compliant chips and locating products containing such chips. FAA officials admit that they still do not know the extent of the problem and admit they are concerned about the potential consequences of microcode glitches.<sup>52</sup>

Not all news is bad. The FAA has taken some important proactive steps. For example, the FAA has embarked on a comprehensive effort to educate the aviation community by establishing a Y2K website, disseminating airport systems lists, and sponsoring "Industry Days."<sup>53</sup> These Industry Days "bring together key stakeholders from all sectors of the aviation industry to raise awareness and work together to solve Y2K problems that are specific to aviation safety and efficiency."<sup>54</sup> The FAA prepared a Y2K International Project Plan in an effort to coordinate with international partners.<sup>55</sup> The FAA reached an agreement with Canada to test data exchanges and interfacing air traffic control systems.<sup>56</sup> The FAA is working with other countries to reach similar agreements. Finally, as a fallback, the FAA is in the process of completing a "Business Continuity and Contingency Plan" for use in the event of any failures that may arise.<sup>57</sup>

## V. AIRPORTS

Airports all over the world are busy trying to assess the impact Y2K may have on their facilities. It has been proven that equipment failure at one airport can cause significant disruptions at other airports. For example, the new Hong Kong airport re-

---

<sup>51</sup> See Willemsen, *supra* note 36.

<sup>52</sup> See Robert Goyer, *January 1, 2000: A Date with Disaster, Flying*, April 1998.

<sup>53</sup> See Federal Aviation Administration's Year 2000 website (visited September 22, 1998) <<http://www.faa2k.com>>; see also Garvey, *supra* note 41.

<sup>54</sup> *Supra* note 44.

<sup>55</sup> See *id.*

<sup>56</sup> See *id.*

<sup>57</sup> See FAA website, *supra* note 47.

cently experienced massive computer problems that had far-reaching effects.<sup>58</sup> It was reported that:

Hundreds of airplanes couldn't land on time, thousands of travelers lost luggage, escalators froze, toilets overflowed, perishable goods rotted in the broiling sun. The anguished Chinese government launched three different investigations as business damage ran into the hundreds of millions of dollars. The reputation of the world's busiest cargo-handling operation was left in ruins.<sup>59</sup>

These flight interruptions alone caused massive delays to connecting airports. Hong Kong's failures are prime examples of what could happen if Y2K hits a large airport and its automated systems.

With these types of consequences in mind, larger airports have been laboring to address Y2K for some time. One such airport is Dallas/Fort Worth International Airport (D/FW), which has been working on the problem since 1996 and is reportedly on target to be fully compliant and verified by October of 1999. Bob Hendricks, acting chief information officer, reports that D/FW is spending nearly ten million dollars to remediate the Y2K problem and to implement contingency plans.<sup>60</sup> At D/FW, contingency plans provide solutions for a full range of potential problems, all the way down to manual operation of computerized systems. Hendricks says, "D/FW has manual overrides on our airfield lighting so, worst-case-scenario, we go out there and flip a switch and the lights come on."<sup>61</sup> Reportedly, Mr. Hendricks has compiled information that he is "anxious to share" with other airports seeking to establish or implement the Year 2000 programs, including information on security systems, lighting, and financial systems.<sup>62</sup>

In September, Richard C. Cullerton, Assistant Vice President for Engineering with the Metropolitan Washington Airports Authority (MWAA) testified before the House Subcommittee on Aviation on the efforts that are underway at the MWAA, which operates both the Ronald Reagan Washington National Airport

---

<sup>58</sup> See Mary Fran Johnson, *Monumental Computer System Foul-Ups Could Be Preview of New Millennium*, COMPUTERWORLD, (August 20, 1998) <<http://cnn.com/tech/computing/9808/20/foulup.idg>>.

<sup>59</sup> *Id.*

<sup>60</sup> See Bremer, *supra* note 19.

<sup>61</sup> *Id.*

<sup>62</sup> *Id.*



and Washington Dulles International Airport.<sup>63</sup> MWAAP participated in a pilot program with the Airline Transport Association (ATA) to identify all airport Y2K systems, trained thirty-one employees in Y2K remediation, inventoried systems, implemented procurement Y2K compliance language in contracts, and worked with external utility systems to achieve mutual preparedness.<sup>64</sup> The MWAAP expects to spend six million dollars on Y2K preparedness.<sup>65</sup>

D/FW and the MWAAP have sizeable resources available to address Y2K problems. Smaller airports and other general aviation facilities may not, and their Y2K readiness is of great concern. Smaller airports "are having difficulty with Y2K compliance because they lack the resources to hire the necessary personnel with the unique expertise to conduct assessments of their existing airport facilities, technology systems or equipment."<sup>66</sup>

In an effort to aid these airports, [the FAA is] proposing an amendment to the FAA reauthorization bill now pending. This amendment would provide authority during Fiscal Year 1999 only for airports to use the Airport Improvement Program (AIP) entitlement grants or State Apportionment Funds to assess all the existing airport facilities, technology systems, or equipment owned by the airport, whether or not such systems are normally eligible task for AIP assistance. This will enable these airports to discover the scope of their Y2K problem. Our estimate is that, with this new authority, airports may use as much as 100 million dollars from their existing AIP resources to accomplish this task.<sup>67</sup>

In addition to AIP funding, smaller airports should join with larger airports to utilize the resources and experiences of other airports and aviation organizations that have the necessary procedures and resources. Numerous organizations have rallied to address airport problems. The FAA has implemented an airport webpage with an emphasis on providing information to such airports.<sup>68</sup> The IATA has surveyed over 150 U.S. airports, and is

---

<sup>63</sup> *Testimony before the House Subcommittee on Aviation, Richard Cullerton, Assistant Vice-President for Engineering, Metropolitan Washington Airports Authority* (September 29, 1998) (transcript available at <[http://www.house.gov/science/cullerton\\_09-29.htm](http://www.house.gov/science/cullerton_09-29.htm)>).

<sup>64</sup> *See id.*

<sup>65</sup> *See id.*

<sup>66</sup> Garvey, *supra* note 44.

<sup>67</sup> *Id.*

<sup>68</sup> *See The Official Website of the Office of Airports* (visited September 30, 1998) <<http://www.faa.gov/arp/arpmain.html>>.

compiling data about Y2K vulnerable systems.<sup>69</sup> IATA has also started performing similar assessments at non-U.S. airports using the same methodology, and its data will be incorporated into IATA's database. The American Association of Airport Executives (AAAE) also prepared a comprehensive airport checklist.<sup>70</sup> These groups have conscientiously determined that sharing related information is critical to facilitate Y2K preparedness for all airports.

Access to Y2K information would facilitate matters at smaller airports, whose resources are limited. Small airports handle most of the country's general aviation (GA), and "GA is the largest single segment of the aviation industry in the U.S., flying approximately 120 million passengers each year."<sup>71</sup> GA "employs approximately 540,000 people nationwide with an annual payroll of more than fourteen and a half billion dollars."<sup>72</sup> Y2K, a substantial problem in general aviation, could be disastrous.

To facilitate an exchange of Y2K information, "Year 2000 Information and Readiness Disclosure Act" was signed into law by President Clinton on October 19, 1998.<sup>73</sup> This legislation is designed to limit liability for sharing information related to Y2K compliance. Specifically, this Act provides:

In a covered action arising under any Federal or State law of defamation, trade disparagement, or a similar claim, to the extent such action is based on an allegedly false, inaccurate, or misleading year 2000 statement, the maker of that year 2000 statement shall not be liable with respect to that year 2000 statement, unless the claimant establishes by clear and convincing evidence, in addition to all other requisite elements of the applicable action, that the year 2000 statement was made with knowledge that the year 2000 statement was false or made with reckless disregard as to its truth or falsity.<sup>74</sup>

The extent to which organizations will rely upon this Act is yet undetermined, and some reports have revealed a pessimism concerning the effect that the Act may elicit. In particular, some commentators believe that the disclosures will only be a

---

<sup>69</sup> See *Y2K-Status.org* (visited September 30, 1998) <<http://www.y2k-status.org/AirTransport.htm>>.

<sup>70</sup> See *Airportnet* <<http://www.airportact.org>>.

<sup>71</sup> *Hearing Charter*, *supra* note 17.

<sup>72</sup> *Id.*

<sup>73</sup> See Year 2000 Information and Readiness Disclosure Act, Pub. L. No. 105-271, 112 Stat. 2386 (1998).

<sup>74</sup> *Id.* at 4(c).

means to publish nonsubstantive information without risk of liability. Hopefully, this pessimism will prove unfounded.

## VI. AIRLINES

The airline industry has always been at the forefront of using computers and automated systems to support their business functions starting with the introduction of the first automated reservations system over thirty years ago. Since then, information technology has been used to support virtually all aspects of the commercial aviation operations, including flight scheduling, passenger check-in, baggage, fueling, maintenance check and cargo screening.<sup>75</sup>

ICAO and IATA began compiling and sharing Y2K information with member airlines long before the Year 2000 Information and Readiness Act was passed. Whether or not they began soon enough is questionable, given that a recent IATA survey revealed that approximately twenty-five percent of IATA member airlines did not believe they will have their computers working properly until "the last half of 1999."<sup>76</sup> In an effort to expedite Y2K remediation for the aviation industry, these organizations planned meetings for the first Thursday of each month at ICAO's headquarters in Montreal, Canada.

The first coordinated meeting was held on July 2, 1998. At that meeting, one of the key concerns voiced was how developing countries would be able to deal with the Y2K bug.<sup>77</sup> Present for that meeting were representatives from the FAA, the United Kingdom, ICAO and IATA. An informal action group was established called The Informal Global Y2K Co-ordination Action Group (IGYCAG), and a charter was drafted.

According to ICYCAG's first newsletter, "[a]ll facets of the international civil aviation community will be encouraged to participate in this working group, including airlines, professional bodies (e.g., IFALPA, IFATCA, ATCA, ACI), the communications industry . . . and regional [air traffic services] providers . . ."<sup>78</sup> Reportedly, IATA member airlines have agreed to fund the program by contributing \$19.7 million to address Y2K. One admirable goal this group formulated was to compile a

---

<sup>75</sup> *Hearing Charter*, *supra* note 17.

<sup>76</sup> Petersen, *supra* note 1.

<sup>77</sup> See INFORMAL GLOBAL Y2K CO-ORDINATION ACTION GROUP (ICYCAG) NEWSLETTER, July 1998 (visited September 22, 1998) < <http://www.icao.int/y2k/newsletterjuly.html> >.

<sup>78</sup> *Id.*

database with pertinent information from various countries, vendors, and other such entities concerning Y2K problems and/or remediation.

During the second meeting of IGYCAG in August 1998, material was presented that IGYCAG had marginal success collecting information from "States, suppliers, vendors, providers, etc. . . . [that] was sensitive in nature and was given with provisos . . . . In this regard, ICYCAG members agreed to work toward gaining authorization to share the information obtained, to the benefit of the international civil aviation community."<sup>79</sup> ICYCAG hopes to succeed in its efforts to get permission to disseminate this information, creating a more global, united approach to a Y2K resolution. It is likely that the Year 2000 Information and Readiness Act may help facilitate this process.

During the third meeting of IGYCAG, interest appears to have increased, and additional organizations were present, including participants from the Airports Council International, IATA, ICAO, the National Weather Service, Société internationale de télécommunications aéronautiques (SITA), and NAV Canada.<sup>80</sup> At this third meeting, it was reported that a "data base of equipment suppliers, and an associated critical equipment list were being prepared by ICAO" would eventually be available on the ICAO website.<sup>81</sup> This is greatly anticipated given that there has been no comprehensive repository established for this information. A working paper was also presented to the group that addressed the issuance of Notices to Airmen (NOTAMS) that may become necessary as a result of Y2K.

Also at this meeting, aviation insurance was a hot topic. Although not identified, a representative from the aviation insurance industry reported that insurance carriers were working to ensure that airlines are taking necessary steps to attain Y2K compliance and "if" the carriers are Y2K compliant, insurance coverage would: "be available as always. There were no intentions to change existing insurance contracts as this would require approval from both parties to such contracts. However,

---

<sup>79</sup> INFORMAL GLOBAL Y2K CO-ORDINATION ACTION GROUP (ICYCAG) NEWSLETTER, August 1998 (visited October 13, 1998) < <http://www.icao.int/y2k/newsletteraug.html>>.

<sup>80</sup> See INFORMAL GLOBAL Y2K CO-ORDINATION ACTION GROUP (ICYCAG) NEWSLETTER, September 1998 (visited October 13, 1998) < <http://www.icao.int/y2k/newslettersept.html>>.

<sup>81</sup> *Id.*

new contracts would be reviewed as necessary and this could, quite possibly lead to exclusions in insurance coverage.”<sup>82</sup>

Other than newsletters from organizations such as IGYCAG and governmental reporting, information on individual airlines is difficult to assemble. It has not been made public, and generally, information has come from newspaper articles. The currency and authenticity of this information is not readily verifiable.

Consequently, the status and operations of the airlines is still undetermined. Most likely they are waiting to assess the readiness of the FAA, international facilities and their own aircraft before making any public pronouncements.

## VII. AIRCRAFT

Aircraft manufacturers and component part manufacturers have been actively testing their equipment for Y2K compliance. Despite their repeated efforts, no comprehensive repository has yet been made public concerning Y2K compliance of aircraft. However, manufacturers have provided information concerning specific aircraft in response to inquiries or have posted information on the internet.<sup>83</sup> The disclosure of this information is and should be made public because without access to this information, neither inspectors nor mechanics will have information they need to evaluate an aircraft's airworthiness.

In order for an aircraft to pass inspection, it must be “airworthy.” Many aviation cases cite a two-prong test for airworthiness.<sup>84</sup> This test is derived from the following provision of the Federal Aviation Act, “The Administrator shall issue an airworthiness certificate when the Administrator finds that the aircraft conforms to its type certification and, after inspection, is in condition for safe operation.”<sup>85</sup>

The Federal Aviation Regulations provides as follows:

---

<sup>82</sup> *Id.*

<sup>83</sup> See, e.g., *Readiness of Boeing Airplanes for Year 2000 Operations* (visited July 21, 1998) <<http://www.boeing.com/commercial/aeromagazine/aero-3textonly/syoltxt.html>>.

<sup>84</sup> See, e.g., *Copsey v. National Transportation Safety Board*, 993 F.2d 736, 738 (10th Cir. 1993); *Morton v. National Transportation Safety Board*, 525 F.2d 1302, 1307 (10th Cir. 1975); *In the Matter of American West Airlines*, FAA Order 96-3 at 29 n. 27 (February 13, 1996).

<sup>85</sup> 49 U.S.C. § 44704(d)(1)(1994) (emphasis added).

(a) Unless sooner surrendered, suspended, revoked, or a termination date is otherwise established by the Administrator, airworthiness certificates are effective as follows:

(1) Standard airworthiness certificates . . . are effective as long as the maintenance, preventive maintenance, and alterations are performed in accordance with Parts 43 and 91 of this chapter and the aircraft are registered in the United States.<sup>86</sup>

The standard airworthiness certificate provides that:

Unless sooner surrendered, suspended, revoked, or a termination date is otherwise established by the Administrator, this airworthiness certificate is effective as long as the maintenance, preventative maintenance, and alterations are performed in accordance with Parts 21, 43, and 91 of the Federal Aviation Regulations, as appropriate, and the aircraft is registered in the United States.

Numerous concerns have arisen relating to whether aircraft equipment that has undergone remediation efforts to correct Y2K problems will qualify as conforming to its type certificate. Repairs to the electronic circuitry, such as replacing an embedded chip, are like any other maintenance repairs. If the equipment cannot be replaced with an approved part number, any repairs made with unapproved parts may render the airworthiness certificate invalid. If other parts are designed or manufactured to correct the problems, but do not have FAA approval, manufacturers may have to seek a Technical Service Order (TSO) or perhaps a Parts Manufacturing Approval (PMA) to allow the substitution. On the other hand, if the equipment is obsolete or cannot be fixed, manufacturers will have to find other solutions, such as upgrading the equipment.

Routinely, information is provided by manufacturers to the FAA describing modifications and upgrades needed for aircraft, and the FAA can either approve or deny the manufacturer's recommendations. This process may, in and of itself, be lengthy because the manufacturer must provide sufficient information to the FAA to substantiate the change, and time is one of the major Y2K impediments. After time for review, the FAA will determine its course of conduct, whether it approves a TSO, PMA, or calls for the issuance of a Service Bulletin, Airworthiness Directive, or Supplemental Type Certificate. Some Service Bulle-

---

<sup>86</sup> 14 C.F.R. § 21.181(a)(1) (1994).

tins have already issued, but there has been very little publication of other identifiable remediation measures.<sup>87</sup>

At some point in the coming months, manufacturers and the FAA will have to reach an immediate assessment of all necessary remediation because year 1999 and 2000 annual inspections will come due. This puts significant pressure on both the manufacturers and the FAA to immediately identify and reach a resolution on how to remediate all identifiable Y2K problems.

## VIII. AIR TRAFFIC MANAGEMENT/NAVIGATION

Navigation needs also warrant immediate attention to ascertain the scope of any date-related programming problems. One such uniquely aviation date-related problem that has already been identified is in the Global Positioning System (GPS), both civilian and military applications. The GPS suffers from an "End of Week Rollover" (EOW) problem.<sup>88</sup> Because of the manner in which the clocks in the equipment operate, they will completely reset after 1,024 weeks of operation. This is scheduled to occur for all receivers and satellites on August 21, 1999.<sup>89</sup> When the clocks reset, some equipment may or may not understand what occurred or how to interpret the new data. As a result, GPS receivers may not be able to compute the reset information, or they may make an attempt to calculate location using information the equipment does not understand. If a GPS receiver has not been properly designed to deal with this change, it is likely to be inaccurate.

There are several sources of information to identify whether or not a GPS receiver is likely to operate correctly. The Department of Defense has been actively testing equipment and posting the results on a website.<sup>90</sup> Additionally, a number of GPS manufacturers have websites that may provide information on their receivers.<sup>91</sup> If internet access is not available, it is recom-

---

<sup>87</sup> See Max Kingsley-June, *Airbus to Cross Finishing Line*, FLIGHT INTERNATIONAL (September 9, 1998) at 62, available in LEXIS, News Library.

<sup>88</sup> See GPS Year 2000 (Y2K) and GPS End of Week (EOW) Rollovers (visited June 26, 1998) <<http://www.laafb.af.mil/SMC/CZ/homepage/y2000/body.htm>>.

<sup>89</sup> See Y2K/EOW Rollover Issues (visited June 26, 1998) <<http://www.laafb.af.mil/SMC/CZ/homepage/y2000/rollover.htm>>.

<sup>90</sup> See *id.*

<sup>91</sup> See, e.g., GPS Manufacturers (visited June 26, 1998) <<http://www.navcen.uscg.mil/gps/geninfo/y2k/gpsmanufacturers/manufacturers.html>> (including addresses, phone numbers, points of contacts, fax numbers and web addresses for over 75 companies).

mended that an inquiry be forwarded to the GPS manufacturer for Y2K compliance verification.

Not only GPS, but all aircraft avionics are by their very nature Y2K suspect. The Civil Aviation Safety Authority (CASA), is so concerned about avionics that its director, Nick Toller, has written to the industry urging operators to take heed:

Computerised[sic] aviations systems, including hardware and software used for aircraft control displays, navigation, communications, engine controls, flight controls, and loading of flight data, could be hit by the Year 2000 (Y2K) problem. "This is not a media beat-up, but the considered opinion of the most informed authorities on the subject," Toller wrote. . . . CASA said large aircraft with integrated avionics systems were most likely to be affected while many small aircraft may not be affected at all.<sup>92</sup>

Because the FAA has the job of making sure that FAA certified electronic equipment will be able to handle Y2K and related rollovers,<sup>93</sup> the FAA says it will be looking at, and testing for compliance, every piece of equipment that might be affected by Y2K issues, including autopilots, flight management computers, flight controls, GPS receivers, surveillance and traffic conflict avoidance, and other navigation and communications equipment.<sup>94</sup> However, as late as April, 1998, the agency admitted in a letter to Congress that it did not have a formal plan "to assess vulnerability of microchips embedded in airborne electronic equipment."<sup>95</sup>

Other avionics are also under the microscope. For example, flight planning programs commonly referred to as "avcomps" have also been under scrutiny lately. Avcomp vendors, like other organizations, are scrambling to assess the Y2K compliance of their products. However, the assessment phase is lengthy, and includes time spent waiting for underlying software manufacturers to respond to inquiries.<sup>96</sup> As expected, vendors communicate an optimism that their programs are, or will be, Y2K compliant. Nevertheless, the only way to know for certain whether any program, including an avcomp, is Y2K compliant or relies on further Y2K compliant underlying programs, is to contact the vendor and get the information in writing.

---

<sup>92</sup> *Aviation Industry Warned about Millennium Bug*, *Ninemsnnews*, August 22, 1998.

<sup>93</sup> See Garvey, *supra* note 44.

<sup>94</sup> See *id.*

<sup>95</sup> *Id.*

<sup>96</sup> See *id.*



## IX. TRAVEL RESERVATIONS

Assuming airports and airlines are fully operational, travelers may have some problems with respect to their efforts to make travel plans. For example, much literature has already been written about the SABRE travel reservation system.<sup>97</sup> SABRE has been one of the uniform systems for making airline and other travel reservations for a number of years. This network is widely interconnected with a host of external computers feeding into it. To address Y2K, SABRE must "replace or repair the hardware and software that support 180,000 terminals that connect to its reservations system," and "pore through 200 million lines of mainframe code."<sup>98</sup> SABRE reportedly hired a remediation company out of Massachusetts early in 1998, in furtherance of its plan to be fully compliant by the middle to the end of 1998.<sup>99</sup>

Other systems, such as the Worldspan, L.P., owned by Delta Airlines, Inc., Northwest Airlines Corp., and Trans World Airlines, have also been reported to be well on their way to being Y2K compliant.<sup>100</sup> However, the steps being taken and the status of those efforts is unknown. After all, it goes without saying that a noncompliant reservation system or a compliant system with noncompliant external data would paralyze the entire aviation system. Further, analysis of the readiness of reservation systems should begin to surface long before January 1, 2000.

## X. INSURANCE

Although reservations and passenger insurance is likewise necessary for airlines and airplanes to operate, even insurance coverage and availability has been affected by Y2K. According to one report:

The Year 2000 exposure facing insurers is in many ways analogous to the huge onslaught of environmental claims that caught most insurers by surprise. When general liability policies were

---

<sup>97</sup> See Thomas Hoffman, SABRE Group Harness Y2K plans, *COMPUTERWORLD*, March 2, 1998 at 31; see also *The SABRE Group* (last modified Jan 21, 1998) <<http://www.sabre.com>>.

<sup>98</sup> See Thomas Hoffman, *supra* note 88, at 33. (Debra Friedman, senior vice-president for Sabre's technology application, reportedly has fixed and at least begun testing approximately ninety-four percent of its systems. This report conflicts with other reports concerning the status of the Sabre system, and the exact status may not be known until the clocks roll over).

<sup>99</sup> See *The SABRE Group Choose GILES 2001 for Century Date-Change Solution*, <[http://www.year2000.com/releases/global1\\_30\\_1998.html](http://www.year2000.com/releases/global1_30_1998.html)>.

<sup>100</sup> See Jennifer Thomas-Bloomberg, *supra* note 23.

written in the 1960's and earlier, the public and the government were only dimly aware of environmental issues and claims for pollution related damages and defense costs were not extensive. As environmental awareness became heightened in the 1970's, the number of pollution claims increased and insurers began to add "sudden and accidental" pollution exclusions to their policies. After the Comprehensive Environmental Response, Compensation and Liability Act (CERCLA) was passed in 1980, insurers sought to strengthen the pollution exclusion by developing an obsolete pollution exclusion. The litigation that ensued to clarify the intent of these exclusions and the insurance coverage available to commercial business exploded and has now cost insurers an estimated \$60 Billion for hazardous waste claims alone. A similar scenario applies to the asbestos litigation. It could now apply to the Year 2000 problem. A common mistake insurers have made is that they did not understand the breadth of coverage the policies could provide for exposures not contemplated at the time the policies were written.<sup>101</sup>

With respect to insuring risks, the exposure is already evident, as there have already been a number of lawsuits filed. In one of the first suits filed, Produce Palace International sued All American Cash Register, Inc. for lost profits and other problems arising out of a Unix Point of Sale System installed by the defendant.<sup>102</sup> The system crashed when a customer trying to use a credit card with an expiration date of "00" completely disabled all ten registers in the office system. Customers walked out and when the plaintiff brought this problem to the defendant's attention, the defendant wanted \$40,000 to correct the problem. The plaintiff sought business interruption damages and costs associated with repairing or replacing its cash registers. That suit was recently settled in the plaintiff's favor.

Other plaintiffs have sought relief from Y2K problems. For example, *Atlaz International, Inc. v. Software Business Technologies, Inc.* was filed in December of 1997 in California state court.<sup>103</sup> This suit involved an accounting software program that was not Y2K compliant. In another suit, *Capellan v. Symantech Corporation*, the plaintiff complained that the Norton Anti-Virus Version 4.0, was not Y2K compliant<sup>104</sup> alleging that the scheduling func-

---

<sup>101</sup> Emily Canelo, *The Reinsurer of the Year 2000*, *Mealey's Year 2000 Report*, April 1998.

<sup>102</sup> See *Year 2000 Lawsuits (Filed and Potential)* (visited July 21, 1998) <<http://www.consult2000.com/litigati.htm>>.

<sup>103</sup> See *id.*

<sup>104</sup> See *id.*

tions in that program do not operate correctly for dates 2000 and later. *Issakson v. Intuit* is a suit alleging problems with the popular software program Quicken, and *Paragon Networks, International vs. Macola* is a suit in which the plaintiffs allege tortious misrepresentation concerning the sale and purchase of an accounting package that advertised "accounting software you will never outgrow."<sup>105</sup> Other suits seek damages for problems with telephone voice activation systems, and most claim unfair or deceptive trade practices.<sup>106</sup>

The litigation has already started. Insurers and underwriters are busy trying to assess the coverage risks, because the issues range from business interruption and shareholder suits to products liability, the risks have been very complicated to analyze. As for aviation insurance, as set forth above, representatives have already reported that the industry hopes to avoid Y2K exclusions, but the trend appears otherwise. In 1997, the London Insurance Market formed "The Millennium Management Group" to deal with Y2K issues.<sup>107</sup> According to Martin Cox, of the British Aviation Insurance Group in London, England, aerospace insurers have developed a plan to assess Y2K compliance of its insureds. To the extent that the insureds demonstrate "that they have taken all reasonably necessary measures to comply with date recognition conformity" then coverage will issue under two different types of endorsements.<sup>108</sup> Otherwise, the policies will contain a date recognition exclusion. These provisions are likely to broaden in use throughout the industry as the time approaches. It has been reported that "Cigna, AIG [Aviation Insurance Group], and AAU [Associated Aviation Underwriters] have already begun notifying clients of Y2K and GPS rollover exclusions and . . . other companies will soon follow."<sup>109</sup>

Not only are insurers taking contractual steps to address Y2K risks, but they have also taken regulatory steps. Legislation was

---

<sup>105</sup> *Id.*

<sup>106</sup> *See id.*

<sup>107</sup> Martin Cox, *Aviation Insurance and the Millennium Bug*, an article published in the 1998 Aviation Litigation Seminar presented by Aviation & Space Law Committee of the Tort and Insurance Practice Section and the Aviation Litigation Committee of the Section of Aviation (October 22-23, 1998).

<sup>108</sup> *Id.*

<sup>109</sup> *Keep Me Covered - The Insurance Companies are Getting Jittery about Y2K and GPS Rollover*, THE AVIATION CONSUMER, November 1998.

recently passed in Australia which allows insure's to engraft a Y2K exclusion into air carrier liability coverage:

Under the Civil Aviation (Carriers Liability) Act, airlines are required to insure each fare-paying passenger for at least \$500,000 against damages arising from accidents and other events. Until recently the only permissible exceptions to the liability insurance were radioactive contamination, nuclear risks, noise and pollution, and war and hijacking. However, since August 11th, [1998] when amendments to the regulations came into effect, airlines have been permitted to fly with insurance that contains a "date recognition exclusion clause." The clause specifically excludes insurance coverage for events caused by the failure of computer systems, integrated circuits or silicon chips in connection with:

- The change of year from 1999 to 2000;
- The change of date from August 21, 1999 to August 22, 1999, (when global positioning satellite counters are due to reset themselves to zero);
- Any other change of year, date, time.<sup>110</sup>

A comprehensive review of all insurance policies' terms and conditions is warranted for potential losses that may occur as a result of the Y2K bug. In addition to aviation policies, this review should include comprehensive general liability insurance, officers and directors policies, and business interruption insurance.

Most comprehensive general liability policies exclude coverage for aviation liability claims. They provide coverage in the event of an "occurrence."<sup>111</sup> "Occurrence" is generally defined in policies as "an accident or event including continuous or repeated exposure to conditions . . . neither expected nor intended from the standpoint of the Insured."<sup>112</sup> The key phrase in this provision is "neither expected nor intended." It is unlikely that a court would find that the failure to diagnose and correct a Y2K problem is unexpected or unintended from the standpoint of the insured. Numerous speakers, including risk management personnel, have concluded that a Y2K failure is something that should have been known to insureds, and a com-

---

<sup>110</sup> Stan Beer, *Air Travelers May Bear Bug Risk*, A.F.R. Net Services Financial Review August 26, 1998.

<sup>111</sup> Katherine B. Posner, *Aviation Coverage in the Year 2000* (1998) available in AirportNet website.

<sup>112</sup> *Id.*

pany's refusal to appreciate the risks involved will not protect it from a denial of coverage.<sup>113</sup>

As for officers and directors liability, care should be given to the potential claims that assert breach of fiduciary duty for failure to remedy the Y2K problem. If a company suffers substantial business interruption and profits, these claims are likely to arise. Additionally, some materials infer that other claims for breach of fiduciary duty may arise from shareholders for company losses.<sup>114</sup>

As for aviation liability insurance, covered claims are those that arise out of the "ownership, operation, maintenance or use (including loading and unloading) of any Aircraft."<sup>115</sup> Generally these policies do not cover first party claims (i.e. those claims made by the insured), but cover personal injury and property damage claims made by third parties. Covered claims must still meet the policy requirements, including the requirement that the injury be caused by an "occurrence."<sup>116</sup>

Aviation products liability insurance may cover products furnished by the insured and "installed in" or "used in connection with" an aircraft. This provides coverage for claims made by the end user, and would likely provide coverage for the failure of navigation equipment and avionics. However, coverage is excluded when the product is "in the care, custody or control of the insured" or where the "occurrence" does not arise out of the handling or use of, or the existence of a condition in the insured's product.<sup>117</sup>

Grounding liability policies provide coverage for "an existing, alleged or suspected like defect, fault or condition affecting the safe operation of two or more like model aircraft."<sup>118</sup> For example, if the FAA is alerted that one or more like aircraft have equipment that does not meet Y2K standards and imposes a grounding order because of that defect, coverage *may exist*. However, it appears that the new policies coming out of the London aviation market may specifically exclude all Y2K related

---

<sup>113</sup> Thomas Reiter, *Policyholders Guide to Coverage for Year 2000 Losses* (March 1998) <<http://www.kl.com/PracticeAreas/y2k/pubs/page2.stm>> Laura Foggan et al., *An Insurer Perspective on CGL Coverage Issues Posed by Potential Year 2000 Claims*, Mealey's Year 2000 Conference, May 1998.

<sup>114</sup> See Cox, *supra* note 102.

<sup>115</sup> *Id.*

<sup>116</sup> Posner, *supra* note 106.

<sup>117</sup> See *id.*

<sup>118</sup> *Id.*

grounding and loss of use claims.<sup>119</sup> Generally FAA mandated grounding may not have coverage under the traditional policies or the new London policies. Consequently, a review of the terms and conditions of this type of policy is recommended.<sup>120</sup>

Business interruption coverage is designed to provide protection for those periods of time when a business is out of operation. Coverage is usually provided for claims involving "Direct Physical Loss or Damage."<sup>121</sup> A potential Y2K claim is more likely to involve lost revenue and lost profits there may be coverage if a business interruption is triggered by a utility outage that causes perishable goods to be destroyed. There may also be coverage if the Y2K problem causes the destruction or loss of electronic data.<sup>122</sup> However, if the business interruption is solely caused by an equipment malfunction and no direct physical loss or damage occurs, there may be no coverage. Once again, a comprehensive audit of the policy is recommended.

Ultimately, a comprehensive review of insurance coverage should be conducted to ascertain what, if any, additional coverage should be requested, or what, if any, exclusions are applicable to the risks.

## XI. BUSINESS APPLICATIONS/MAINTENANCE

In addition to specific aviation-related issues, there is another more insidious and likely Y2K problem. It concerns one of the most basic services upon which everyone relies: utility services—particularly, electric utilities. If utility systems fail, computers will shut down, fax machines will not operate, telephones will not work, and a host of other services will be disrupted. The complex network of supply, delivery, service, repair, and management of all industries, including aviation, could grind to an immediate halt. Recent seminars have indicated that major utility companies are having difficulty identifying their Y2K problems, locating, testing, and replacing problematic embedded chips, and certifying that their systems are Y2K compliant.

Many utility plants are operated by embedded control systems that use computers and sensing devices to regulate the flow of

---

<sup>119</sup> Cox, *supra* note 102.

<sup>120</sup> See *id.*

<sup>121</sup> *Id.*

<sup>122</sup> See *id.* (citing Magnetic Data, Inc. v. St. Paul Fire & Marine Ins. Co., 430 N.W.2d 483 (Minn. Ct. App. 1988)).

electricity.<sup>123</sup> Water pumping and distribution facilities and waste-water-treatment facilities also use similar equipment. To resolve the Y2K problem, testing the computers in these systems will not be sufficient. Exhaustive efforts must be made to locate all embedded processors to negate the possibility that the sensing devices themselves could fail.

According to Rick Cowles, an electric utility industry analyst, not one electric company has started a serious remediation effort on its embedded controls. Not one. Yes, there has been some testing going on, and a few pilot projects here and there, but for the most part it's still business as usual as if there were 97 months to go, not 97 weeks.<sup>124</sup>

The millennium bug will likely cause periodic utility failures that are caused in whole or in part by Y2K, but failures are not likely to be systemwide because in many instances a defective service line can be isolated and service rerouted. Therefore, utility failures are certainly an issue of concern, but short-term isolated failures are more likely to be a temporary nuisance. If runway lights shut down at an inopportune time, however, the results could be catastrophic.

## XII. REMEDIATION

Before effective remediation can begin, the world must realize that the Y2K issue is a "business continuity problem,"<sup>125</sup> a "communications problem, . . . a utilities problem, a logistical problem, a national and international business problem, and a governmental problem."<sup>126</sup> To address the problem, the scope of activities, businesses, equipment, and even our recreation must be assessed. Once this realization has been made, each person and company must make a Y2K assessment.

Great mysteries remain concerning how some companies are addressing the Y2K issue. Large companies with information technology departments have implemented large comprehensive plans, but there seems to be very little activity for small businesses or individuals. A representative from the Information Technology Association of America (ITAA) lobbied Congress to

---

<sup>123</sup> Rick Cowles, *Industry Gridlock*, (February 27, 1998) <<http://www.y2ktimebomb.com/PR/RC/rc9808.htm>>.

<sup>124</sup> *Id.*

<sup>125</sup> Tim Wilson, *New Y2K Tack: Damage Control*, *Internet Week* (April 6, 1998).

<sup>126</sup> *About Time: Managing the Y2K Problem in Local Government*, *Texas Guidebook 2000* (visited August 1998) <<http://www.life.state.tx.us/y2k/resources/guide2000.htm>> [hereinafter *Guidebook*].

intervene on behalf of small business. ITAA President Harris Miller testified before Congress in support of a small business intervention program. Fortunately, the government and the U.S. Small Business Administration (SBA) responded by creating a twenty-four hour help line to provide information by fax on ways to avoid Y2K computer problems. The SBA provides assistance from auditing to remediation. They have prepared a number of forms and other resources for small businesses. The SBA also created a website<sup>127</sup> that provides information including a self-assessment test that business owners can take. Some states have also developed similar resources. One such resource for fundamental checklists and assistance can be found in the *Texas Guidebook 2000*, which was commissioned by the State of Texas, Office of the Governor.<sup>128</sup> These are just two of the many resources that are available to businesses (large or small) and individuals. The actual number of organizations is incredible.

### XIII. GENERAL ACCOUNTING OFFICE PROCEDURE

Getting started is the key. The GAO has outlined one simple process. It includes five steps: awareness, assessment, renovation/conversion, testing/validation, and implementation.

#### A. AWARENESS

In the awareness phase, each company should come to understand that Y2K is not merely a computer problem. It is a business management concern and it involves a reasoned analysis of each company's critical functions. Awareness is vital, and it requires a recognition of the scope of potential problems, an understanding of the scope of the potential effects of the business, and a publication of the issues involved. No one can rest on the assumption that someone else will fix the problem. It will take a coordinated effort of every department and individual to identify where the problems may lay.

Some aviation companies have implemented effective Y2K awareness programs. For example, one company has designated a Year 2000 Program Manager, an Information Technology Year 2000 Team Leader, a Product Integrity Team Leader, a Customer Contact Team Leader, a Supply Chain Team Leader, and a Manufacturing & Facilities Team Leader. These various enti-

---

<sup>127</sup> See <<http://www.sba.gov/y2k>>.

<sup>128</sup> See *Guidebook*, *supra* note 121.



ties provide insight into the scope of awareness that is needed at all levels.

## B. ASSESSMENT

Once Y2K is recognized as a current resource allocation and business coordination issue, it must be thoroughly assessed. This step begins with an inventory of computer equipment including hardware and software, office equipment (including but not limited to communications equipment, telephones, facsimiles, copy machines, and audio/visual equipment), buildings and facilities (including but not limited to security systems, heating/cooling systems, and elevators), tools/equipment, avionics/nav aids, critical supplies, and critical vendors.

A thorough inventory must be prepared. This inventory will reveal those items that are vital for continued operations. In some instances a third party may be needed to prepare the inventory and assessment. For aviation-related entities, there are a number of trade associations that may provide this service.<sup>129</sup> Alternatively, the SBA may be able to provide assistance.

Once the inventory is complete, the items identified should be prioritized. Those pieces of equipment, supplies, and vendors that are necessary for operations should be identified. For example, if an FBO would shut down if the fuel were not delivered on a daily basis, then an in-depth investigation should be undertaken to determine the amount of fuel needed for continued operations, whether the supplier will be able to continue deliveries, and what alternative sources may be available in the event of a supply interruption. Additionally, the FBO should identify essential equipment in the shop to determine whether it may have an embedded chip and ascertain what alternatives may be available in the event the equipment fails. A comprehensive assessment should also identify those items no longer useable or serviceable, those items that are not Y2K compliant, those items that should be upgraded or replaced, and those that require remediation.

A very recent inventory of vendors has been assembled by Electronic Data Systems (EDS), which unveiled a website for "Vendor 2000" information.<sup>130</sup> One should also monitor the

---

<sup>129</sup> See The FAA's internet website index (visited September 22, 1998) <<http://www.faa2k.com/html/relatedmiddle.html>>.

<sup>130</sup> (visited October 13, 1998) <<http://www.eds.com/vendor2000>>.

ICAO website, as it plans to publish similar information.<sup>131</sup> For aviation related equipment, the FAA has prepared a "Y2K Airfield System List," which is an inventory of equipment ranging from access controls to communication to weather systems.<sup>132</sup> This broad inventory list would be a useful place to start.

Not only should existing equipment, services, and vendors be assessed for compliance, but any new equipment acquisitions and service contracts should be assessed as well. The U.S. government has implemented standard policy language that requires all governmental contracts to "warranty" Y2K compliance:

The contractor warrants that each hardware, software, and firmware product delivered under this contract and listed below shall be able to accurately process date data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, including leap year calculations, when used in accordance with product documentation provided by the contractor, provided that all listed or unlisted products (e.g. hardware, software, firmware) used in combination with such listed product properly exchange date data with it. If the contract requires that specific listed products must perform as a system in accordance with the foregoing warranty, then that warranty shall apply to those listed products as a system. The duration of this warranty and the remedies available to the Government for breach of this warranty shall be as defined in, and subject to, the terms and limitations of the contractor's standard commercial warranty or warranties contained in this contract, provided that notwithstanding any provision to the contrary in such commercial warranty or warranties, the remedies available to the Government under this warranty shall include repair or replacement of any listed product whose non-compliance is discovered and made known to the contractor in writing within ninety (90) days after acceptance. Nothing in this warranty shall be construed to limit any rights or remedies the Government may otherwise have under this contract with respect to defects other than Year 2000 performance.<sup>133</sup>

The language exemplifies the type of clause that could be incorporated into new acquisition contracts, but there are wide

---

<sup>131</sup> (visited October 13, 1998) <<http://www.icao.org/y2k/index.html>>.

<sup>132</sup> (visited October 13, 1998) <<http://www.faa.gov/arp/arphome.htm>>.

<sup>133</sup> Barry Tate, International Aircraft Transport Association, *Year 2000 Countdown to Chaos?* (visited September 30, 1998) <<http://www.iata.org/y2k/articles.htm>>.

variations of contract clauses that have been drafted into contracts.<sup>134</sup>

### C. RENOVATION/CONVERSION

After an inventory and assessment has been completed, businesses should plan for renovation and conversion of systems. Funds should be allocated for this phase of the program, because this phase may include the costs of upgrading or repairing noncompliant purchase of upgraded systems, upgraded software, or simply replacing some equipment. Many software programs have patches available on the internet from the software developer to upgrade them to resolve Y2K problems. If software upgrades are needed, all information on the computer should be backed up and saved before any upgrades are installed. If necessary equipment is near the end of its useful life, a newer, Y2K compliant model should be considered. Because all sources of data transfer are unusually susceptible to problems, outgoing and incoming information should be monitored for date-related information.

If non-compliant software has been identified, remediation plans should be undertaken with care and caution. Many companies are considering the use of overseas Y2K programmers. Programmers have been sought in South America, Canada, India, and Africa. If international programmers are retained, the company should be careful to determine if any cryptographic software applications are involved. This includes wire-transfer systems, communication systems, or other software application where the process date is encrypted for security purposes. There are some encryption software programs that are prohibited from being exported, even for remediation purposes.<sup>135</sup> To the extent that remediation requires forwarding of the program outside the country, there may be some federal restrictions and penalties to be avoided.

---

<sup>134</sup> Jeff Jinnett, *Contracting Issues with Customers and Vendors, Understanding, Preventing and Litigating Year 2000 Issues What Every Lawyer Needs to Know Now*, 506 P.L.I./Pat 77 Law Institute (1998); see also 1 TAC §201.13(e).

<sup>135</sup> Jeff Jinnett, *Legal Issues Concerning the Year 2000 Computer Problem: An Awareness Article for the Private Sector, Year 2000 and the Millennium Bug - the "Jurassic Park" of Business or Hoax of the Century* address before the Committee on Corporate Counsel ABA Section of Business Law 1998 Annual Meeting, Toronto.

#### D. TESTING/VALIDATION

Finally, after the equipment, software and/or services are repaired, they should be tested. Testing should be conducted on all operations as comprehensively as possible. “[M]any airlines have already conducted a detailed analysis of what is required to make the necessary conversions [and] have found that the costs and efforts are likely to be significantly less than the ‘scare’ figures quoted and also less than for some other industries.”<sup>136</sup> Testing should not be done in a vacuum. For example, the comprehensive scope of the FAA’s equipment requires a coordinated schedule of end-to-end testing. This requires a test procedure that flows from facility to facility across the nation to assure operational continuity. Most organizations will not require this type of testing process. However, testing is an important phase and it should include external sources of data to the extent possible.

#### E. IMPLEMENTATION

Once testing is completed, the software and equipment should be implemented as soon as feasible. Having the software equipment in place before January 1, 2000 is one way to provide as much protection as possible.

### XIV. CONTINGENCY PLANS

Finally, contingency plans should reflect a reasoned approach to a company’s unique needs, although it is impossible to prepare a comprehensive contingency plan that will meet the needs of all companies. As was aptly discussed for flight departments:

The size and complexity of each corporate flight department will dictate the degree of impact of the Millennium Bug. Flight departments that depend heavily on third-party vendors for scheduling/dispatching, maintenance tracking and flight following services will have to discuss the implications of the bug with each vendor. Flight department information technology managers should document all Y2K assurances provided by vendors . . . Finally, consider your flight department’s liability if, despite everyone’s efforts and good intentions, essential computer systems fail. If air traffic services are severely affected after all, it might be best to have some contingency plans in place so

---

<sup>136</sup> *Id.*

that travelers won't be stranded if you can't get to them on schedule.<sup>137</sup>

Contingency plans depend upon the business. These times may require assembling manual data (maps, charts and such) to have available in the event access to flight planning programs is not an option. The plan may be simply to have additional maintenance supplies on hand in the event there is a temporary interruption with vendors and/or have additional cash available in the event there is a problem with check-cashing services or ATMs. Overall, the needs of the individual, the department, the business, and the vendors should be assessed to determine what services are essential to continued operation, and a plan should be put in place in the event of an interruption.

## XV. CONCLUSION

In short, Y2K is not the end of aviation as we know it. It is a global opportunity to upgrade outdated equipment and software. As it has always been, change is not welcome by some and is profoundly anticipated by others. Many in the aviation industry have already upgraded equipment, surveyed networks, assessed reliability, and evaluated efficiency. Y2K is painful, but it is survivable. People have a unique capacity to rise to the occasion, even if the occasion is Y2K. While there will likely be some interruptions in the normal course of affairs, and some may be fairly major, the aviation industry, which has always been a leader in technological advancements, will likely respond by adopting new policies and procedures, streamlining operations, and reassessing risk management. Aviation will continue, and the bug will eventually be eradicated. The extermination of this problem will likely result in a more global approach to problem solving and information sharing. As many aviation war heroes can attest, aviation alliances can begin with shared experiences. Y2K may be just such an experience.

---

<sup>137</sup> Mal Gormley, *Y2K and Business Aviation*, BUSINESS AND COMMERCIAL AVIATION, July 1998, at 68.