Pennsylvania House Judiciary Committee
HB 2273 & HB 2406 / year 2000 indemnification

Prepared Testimony of John D. Berkheimer
CEO of Berkheimer Associates
Pennsylvania local tax administrators

Thursday July 9th , 10:00 a.m.

Full Text of Testimony

Mr. Chairman and distinguished members of the committee:

My name is John Berkheimer, I am the Chief Executive Officer of Berkheimer Associates, a firm that has specialized in the administration of local taxes for school districts and municipal governments throughout the Commonwealth since 1946. I appreciate the opportunity to testify today on the issue of Year 2000 indemnification. The title of my remarks today is *Year 2000: We need remediation, not retribution.*

Conclusion:
The functions performed by elected and appointed tax administrators in maintaining the flow of income to local government is no less important to the safety and infrastructure of every locality, than the Pennsylvania Department of Revenue is to the State. Without the certainty provided by specifically delineated indemnification there is, in my opinion, significant risk that potential problems arising from Y2K may not be adequately addressed, or worse, not addressed at all. Local tax offices will be unable, unwilling or otherwise cease to function under the dual burden of actual problem remediation and defending against causes of action resulting from real or perceived disruption. In other words, if the impact of events precipitated by Year 2000 problems does not halt local government operation.... left unchecked, the litigation aftershock most certainly will.
The result of such a breakdown will be a lack of predictable funding to grass roots government necessary to the provision of "mission critical" services for constituents, at a time when they are most needed.

Background on Y2K problem:

The parallels between the disease, cancer and the Y2K problem are remarkable. Each can exist for a long time unnoticed. The symptomatic onset of both can be rapid and painful. Neither go away of their own accord; and each have the capability to be deadly. Many armed with a layman's knowledge of cancer remain baffled that so many years after putting a man on the moon, we cannot conquer this killer. One of the reasons is that the umbrella "cancer" covers many manifestations. In fact, cancer is many diseases. I submit that the Y2K computer problem is likewise, not one problem but literally millions, that cannot simply be left to the techo-nerds to solve. Calling in an army of bespectacled "pocket protector" types will not stop the problem from happening.

My views are shared by some internationally respected experts, not the least of whom is Dr. Edward Yardeni, Ph.D. Chief Economist for Deutsche Bank Securities. Dr. Yardeni ias been a frequently relied upon authority during numerous Federal Government hearings on the subject. He has distilled the building avalanche of data on the problem into some very insightful information. I have attached a copy of his report released just 8 days ago as appendix I to this testimony.

Does Anybody Really Know What Time It is ???

Since hard data on the local level is somewhere between scarce and non-existent, an extrapolation from the progress and events experienced by the Fed's can be of some guidance. The following is an excerpt from Dr. Yardeni's report on the subject of the OMB (Office of Management and Budget) report released in mid June:

> In May 1997, OMB reported that roughly 21% of the government's mission-critical systems were ready for Y2K. A year later, approximately 40% of 7,336 such systems were compliant. Unless remediation progress improves dramatically, a significant number of mission-critical systems will fail in 2000. No one is even assessing the status of the 1,020 mission-critical systems that are being replaced. These are especially vulnerable to missing the deadline, since new Information Technology systems are rarely finished on schedule. The fifth report observed:
>
> 1) Nine of the 24 federal agencies have renovated less than 40% of their vital systems,with two having fixed less than 50%.
> 2) Five agencies (Department of Defense, Health and Human Services (HHS), Justice,Transportation, and Treasury) had not even completed the initial

assessment phase, nearly a year behind OMB's government-wide target of June 1997.
3) Only 11 of the 24 agencies had completed inventories and/or assessment of their telecommunications systems.
4) Only six reported that they had completed inventories and/or assessment of their embedded systems.

Given the above timeline and degree of progress or lack thereof consider this. The number of working days remaining to 1 January, 2000, [allowing for annual leave, a few sick days and public holidays] are approximately 340. If a small or medium size enterprise commits 10% of its time to this project, only 34 days remain to completion. I think you get my point.
In my opinion, we are beyond the juncture where any solution or group thereof will eliminate the possibility of disruption. The deadline is one that cannot be moved. There simply is not enough time to identify, remediate code and test prior to January 2000.

The time has come to insure that correction of the inevitable cascade of problems, not able to be solved in time, will be a series of positive steps forward to resolution and not a legal admission of guilt. There is no time left to complete doing things right..... now we must resolve to do the right thing. Cut the legal mercenaries out of an already complicated equation to insure the most rapid recovery possible from January 2nd 2000 going forward

Specific language we suggest be added to **HB 2273** and **HB 2406** to provide for uninterrupted local revenue collection is included in Appendix II of this testimony.

APPENDIX I

Deutsche Bank Research

US Equity Research

Dr. Edward Yardeni, Chief Economist
Phone: (212) 469-5715
Fax: (212) 469-5725
E-Mail: yardeni@ix.netcom.com
Web Site: http://www.yardeni.com/

June 29, 1998
#23

THE Y2K REPORTER

Press embargo until 10 am e.s.t. June 30, 1998

THE 70% PROBLEM

Getting Late. I can no longer say with any confidence that there is enough time to avoid a severe global Y2K recession. The fact is, there are only 550 days left, and only 377 business days until judgment day for our computers on January 1, 2000. Progress is occurring, but not as fast as the year 2000 is approaching, in my estimation. At least some vital computer systems in government and business are likely to malfunction because they will not recognize that "00," in the commonly used two-digit year field, is 2000, rather than 1900.

The resulting disruptions in the flow of information are likely to cause a global recession in the same way as did disruptions in the supply of oil during the 1970s. Therefore, I am raising the probability of a global recession—one that could be as severe as the 1973-74 downturn, maybe worse—from 60% to 70%. In the United States, real GDP could fall 5% from peak to trough over a 12-24 month period, starting late in 1999. On a worldwide basis, real GDP could fall by $2 trillion. Nominal GDP might decline even more if the global recession causes deflation, or falling prices.

There are three major reasons why I am raising the probability of a global recession:

1) The response to the Year 2000 Problem from our global leaders has been pathetic. There is no leadership coming from the United States or any other of the G8 nations. They are doing virtually nothing to increase global awareness, to accelerate the pace of remediation, or to prepare for the potential failure of vital systems.

2) The US government continues to make progress, but the pace is too slow. No one is setting national priorities and preparing national contingency plans. Key government regulators—including the Federal Communications Commission, the Securities & Exchange Commission, the Federal Energy Regulatory Commission, and the Nuclear Regulatory Commission—all admit that even they don't have the necessary information to assess the gravity of the situation. It is widely assumed that companies will be ready for the century date change. However, given the lack of adequate disclosure, this may be a naively optimistic assumption.[1]

3) There is virtually no information available on progress outside the United States. This is because the level of awareness is dangerously low in most countries. The bits of information that are available suggest that many government agencies and business entities around the world are at risk of failing to fix 100% of their mission-critical systems in time.

---

[1] See my June 10, 1998 Congressional testimony on this subject at http://www.senate.gov/~banking/98_06hrg/061098/witness/yardeni.htm. A complete database of Y2K disclosure statements from the SEC filings of the S&P 500 companies is available at http://www.yardeni.com/cyber.html#Y1.19

Waiting For Godot. I still hope that a cooperative global crash program to fix Y2K, and to prepare for inevitable disruptions caused by some failures, will reduce the recessionary impact of the Y2K forces heading our way. In my April 7, 1998 keynote speech, "Time To Declare War On Y2K," at the Year 2000 Roundtable of central bankers and banking regulators sponsored by the Bank for International Settlements in Basle, Switzerland, I said, "I probably will raise the odds of a global recession closer to 100% if our leaders do not declare that Y2K is their top priority at the next G8 summit."[2] In my speech, I presented a seven-point global Y2K strategic proposal for the G8 leaders. (See Appendix I.) The G8 leaders met in mid-May 1998 and issued a communiqué that acknowledged the seriousness of Y2K, but failed to mention any serious next steps to deal with the problem. Indeed, Y2K was discussed as point No. 25 in the 25-point communiqué.

In the United States, I believe that the efforts of the President's Y2K Conversion Council are dangerously inadequate. The council's energies are concentrated on fixing the problem on an agency-by-agency basis in the federal government. There is no effort to set national priorities and goals, or to prepare national contingency plans. The council does not even have the authority to collect the information necessary to assess the seriousness of the problem. At a minimum, the council must work to ensure the functioning of vital utilities, including electricity, gas, water, sanitation, telecommunications, and public safety. At this time, the council simply has no first-hand knowledge of whether any of these systems will experience significant disruptions in 2000. It has no way of even monitoring the situation.

Scheduled To Fail. I previously raised the odds of a global recession from 40% to 60% on March 16, 1998, after reading the fourth US federal agency Y2K progress report compiled by the Office of Management and Budget (OMB) for the three-month period through February 15, 1998. The fifth report was released in mid-June.[3] It is alarming, and is one of the reasons why I am raising the odds of a global recession.

In May 1997, OMB reported that roughly 21% of the government's mission-critical systems were ready for Y2K. A year later, approximately 40% of 7,336 such systems were compliant. Unless remediation progress improves dramatically, a significant number of mission-critical systems will fail in 2000. No one is even assessing the status of the 1,020 mission-critical systems that are being replaced. These are especially vulnerable to missing the deadline, since new Information Technology systems are rarely finished on schedule. The fifth report observed:

1) Nine of the 24 federal agencies have renovated less than 40% of their vital systems, with two having fixed less than 50%.
2) Five agencies (Department of Defense, Health and Human Services (HHS), Justice, Transportation, and Treasury) had not even completed the initial assessment phase, nearly a year behind OMB's government-wide target of June 1997.

---

[2] http://www.yardeni.com/y2kreporter.html
[3] http://www.cio.gov/598rpt.html

3) Only 11 of the 24 agencies had completed inventories and/or assessment of their telecommunications systems.
4) Only six reported that they had completed inventories and/or assessment of their embedded systems.

Tears For Tier 1. OMB categorizes agencies in three tiers. In the fifth report, Tier 1 agencies, in which there is insufficient evidence of adequate progress included Defense, Education, Energy, HHS, Transportation, and AID. Only 31% of systems are compliant in Tier 1. Tier 2 includes nine agencies, where OMB sees progress, "but also has some concerns." Tier 3 agencies are in good shape. The situation is so grave in the first two tiers that OMB now wants monthly reports from these agencies beginning August 1, 1998.[4]

Progress Report

	Number of mission critical systems	Number of compliant systems	Percent complete	Official estimated cost to fix (billion)	Agencies in trouble
Feb '97	na	na	na	$2.3	0
May '97	7,649	1,598	21	$2.8	0
Aug '97	8,562	1,646	19	$3.8	5
Nov '97	8,589	2,296	27	$3.9	7
Feb '98	7,850	2,716	35	$4.7	6
May '98	7,336	2,913	40	$5.0	6

Source: Office of Management & Budget

The Check Is In The Mail. OMB is especially concerned about the Financial Management Service (FMS) in the Treasury Department. This agency writes most of the checks issued by the federal government.

> Greater progress is needed in FMS, particularly with respect to the Government On-line Accounting Link System (GOALS), which supports 18 separate financial management applications used by the agencies. The GOALS system has yet to be fully assessed for year-2000 conversion; if the system is not made compliant, the accuracy of government-wide payments, collections, debt management, and accounting information could be compromised.

[4] The FAA's website includes a monthly progress report. http://www.faay2k.com/html/news.html

In June 1998, a House subcommittee was considering transferring check-writing responsibilities for Social Security retirement and disability payments from the Treasury to the Social Security Administration. Even if they do so, there could still be payment problems if telecommunication systems malfunction, since 65% of the payments are deposited electronically.[5]

DEFENSE: GOOD NEWS!?

Strangegloves. In my April 7, 1998 Basle keynote address, I said, "Military leaders of the United States, other NATO members, and Russia must jointly assess the risk of an accidental nuclear missile launch or a provocative false alarm. They must rapidly develop a fail-safe joint communication and intelligence network to eliminate any such risk." According to a June 12, 1998 Reuters dispatch, US Defense Secretary William Cohen offered Russian Defense Minister Igor Sergeyev American expertise and ideas to help them cope with Y2K.

Nightmare Scenario. On June 4, 1998, in a hearing before the Senate Armed Services Committee, John Hamre, Deputy Secretary of Defense, testified, "We plan to field a proposal this summer to ensure exchange of vital nuclear command and control information with other nuclear states." Mr. Hamre said that Russia's early warning system is "fragile." He added that the Pentagon is likely to share early-warning data from US satellites with other countries, including China. Here are some more unnerving excerpts from his testimony:[6]

1) "Our concern is that Russia and China have only a very rudimentary understanding of the Year 2000 problem, which is why we need to reach out to them to make sure they have custodial confidence in their own systems."

2) "We're very concerned, for instance, that the military leadership in Russia right now is coping with serious funding constraints. They are increasingly falling back on nuclear weapons to safeguard their national security; their early-warning system is fragile; and they don't have any program to deal with the year 2000."

3) "We don't want to enter into the nightmare scenario where everyone's screen suddenly goes blank. That would be a very uncertain and worrisome environment for all of us. Frankly, I think we'll be lucky if on January 1, 2000, the system just doesn't come on, because then we'll know we have a problem. Our bigger fear is going to be that the system seems to work fine, but the data are unreliable. That's a far worse problem."

---

[5] *Federal Computer Week*, June 16, 1998.
http://www.fcw.com/pubs/fcw/1998/0615/web-ssa-6-16-1998.html

[6] James Kitfield, "The Pentagon's Nightmare Scenario," DAILY BRIEFING, *National Journal*, June 22, 1998.

4) "We've also shifted from largely dedicated defense communications systems to commercial networks. So if Ma Bell's or Bell Atlantic's system fails on Year 2000, we're going to have mission failure, and I don't have any control over that."

5) "I would be the last person to suggest we're not going to have some nasty surprises, because I definitely think we will. This is going to have implications for American society and the world that we can't even comprehend."

Still think I am overly alarmed?

Friendly Fire. The fifth OMB progress report included the Defense Department in "Tier 1" agencies where there is insufficient evidence of adequate progress:

> The Department has a massive year 2000 challenge which must be accomplished on a tight schedule. Since its February report, progress has slowed. The percentage of compliant mission critical systems has only increased from 24% to 29%, the percentage of mission critical systems being renovated has only increased from 53% to 58%, while the percentage of mission critical systems that has completed implementation has increased from 9% to 17%. At this pace, the Department will not meet its goals and complete its work on time.

AIRLINES: GOOD NEWS!?

"I Believe I Can Fly." Reuters, in a June 9 dispatch, reported that top aviation officials, at their annual general meeting of the International Air Transport Association (IATA) in Montreal, were very confident that their industry would crush the millennium bug:

1) A Boeing executive claimed that after an exhaustive search for any flight safety issues related to Y2K in Boeing aircraft systems, none were found.

2) Notwithstanding previous press reports to the contrary, the general director of IATA said none of his 258 member airlines had informed him that they might not operate on January 1, 2000, because of safety concerns.

3) Jane Garvey, the head of the US Federal Aviation Administration (FAA), said she would be in the air over the United States on January 1, 2000. She added, "Right now, all the lines of (FAA computer) code that need to be fixed are being fixed. Of the 430 mission-critical systems, 141 are already Y2K-compliant." The rest she told Reuters would be ready September 30, 1998!

Scrounging For Spare Parts. Unfortunately, Ms. Garvey's upbeat assessment does not jibe with the findings of the OMB's fifth quarterly progress report, which specifically notes that "the FAA is at significant risk." The remaining tasks are daunting:

> It needs to determine priorities for system conversion and replacement based on systems' mission criticality; develop plans for validating and testing all converted or replaced systems; and continue working to develop realistic contingency plans for all business lines to ensure the continuity of critical operations, including the availability of critical telecommunications support.

Most amazingly, the FAA was only starting to replace its HOST computers—the backbone of en route air traffic support—"to guarantee an adequate supply of spare parts for the remaining computers." The FAA was still assessing the potential vulnerability of the system's micro-code. It was also "validating the feasibility of a date roll-back as one of its potential contingency plans."

To its credit, the FAA has a website that includes a monthly progress report. The latest one through April 17, 1998, shows that the air traffic control system has 57% of its mission-critical systems compliant and fully operational, and another 15% have completed the renovation process. Contrary to OMB's concerns, the FAA claims that the HOST system will be completely renovated by June 30, 1998.[7] The entire system will be compliant by June 30, 1999, according to the FAA. I hope so, but why is there such a huge discrepancy with OMB's assessment?

TELECOM: GOOD NEWS!?

Reach Out And Touch Someone. The OMB is clearly worried that the FAA could be vulnerable if telecommunications systems fail. Maybe there is no reason for concern. *The Star Ledger*, June 13, 1998, reports that AT&T expects to finish most of its Y2K project by the end of this year. Only about 20% of AT&T's Worldwide Intelligent Network required software updates. The most vulnerable items were high-capacity switches, signal transfer points, switches and routers for Internet service, and data transmission lines.

On June 16, 1998, a subcommittee of the House Ways and Means Committee held hearings on Y2K and telecommunications.[8] AT&T's Year 2000 Program Management Vice President John Pasqua testified, "I'm pleased to report that—through May of this year—we have assessed 91% of our application lines of code, repaired 72% of those that needed modification, and application-certified 40%." AT&T relies on the regional bell operating companies (RBOCs) to transfer long-distance calls to homes and businesses

[7] http://www.faay2k.com/html/news.html
[8] http://www.house.gov/ways_means/oversite/ov-18wit,htm

through their local networks. There are more than 1,400 telephone companies in the United States. However, the largest 20 phone companies provide service to 98% of US phone lines.

"I Have Been Told." In his Congressional testimony on June 16, 1998, Michael K. Powell, a commissioner of the Federal Communications Commission (FCC), said, "I have been told that US equipment manufacturers have already tested and fixed most of their products." Most products have been made available to customers.

Mr. Powell assured his Congressional audience that the "carriers report that the manufacturers' schedules will enable them to meet their compliance objectives." Furthermore, based on information provided to the FCC by the carriers, they should be completing their Y2K projects by late 1998 or early 1999. Mr. Powell is the point-man on Y2K issues at the FCC. Yet, at the time of his testimony, he had been at the FCC only seven months. In his testimony, he observed that "our power to force carriers, manufacturers, and telecommunications users to address the Year 2000 problem is limited." Mr. Powell noted that companies are reluctant to divulge information due to concerns about liability.

Dial Tone? Joel C. Willemssen also testified on Y2K telecommunication issues on June 16, 1998 before Congress. He is a director of the US General Accounting Office, which audits federal agencies for Congress. He noted that the White House established a telecommunications working group, which had its first meeting on April 29, 1998. He bemoaned that with less than 19 months remaining, "no one currently has an overall assessment of the degree of Year 2000 risk in the telecommunications infrastructure." Even more alarming is that there is no national coordinated oversight of this vital system.

Mr. Willemssen included a table showing the Y2K-compliance status of the 12 major carriers. The information, showing that the networks should be ready by the end of 1998, was collected from company websites, or telephone interviews with carrier representatives. It was not independently verified.

If the carriers achieve their goals in time, then we will get a dial tone in the United States when we pick up the phone on January 1, 2000. Despite their assurances, I have some serious doubts about this happy scenario. There are even more reasons to doubt that overseas calls will connect. The following table shows the results of a State Department survey of foreign carriers through March 1998. The department received information from 113 countries, of which 22% expected to be compliant by the end of this year, 23% expected to be ready by December 1999, 29% stated they are addressing Y2K but were having problems, and 26% were unaware of or had not begun to address the problem.

I have to conclude that it may be impossible to place calls to some very important countries in 2000. This could seriously damage world trade, and disrupt the system of global outsourcing that is an integral part of just-in-time manufacturing in the United States and around the world.

Global Telecommunications Survey through March 1998

Region	Compliance expected by the end of 1998	Compliance expected by the end of 1999	Addressing Year 2000, but having problems	Unaware or not begun	Total
Central and South America	4	2	4	5	15
Europe and Canada	8	15	9	9	41
Africa	2	1	10	9	22
East Asia and the Pacific	8	6	5	4	23
Near East and South Asia	3	2	5	2	12
Total	25	26	33	29	113
Percentage	**22**	**23**	**29**	**26**	**100**

Source: US State Department

INVESTING FOR Y2K RECESSION

A Defensive Equity Strategy. In a Y2K scenario, corporate earnings are likely to fall dramatically, but so are interest rates. I expect that both the federal funds rate and the 30-year Treasury yield could fall to 3% in 2000. For the stock market, the drop in rates should offset some, but not all of the bad news on earnings. I expect that stock prices could fall at least 30%. I am not sure when investors will start to discount Y2K in stock prices, but it will be within the next 12 months, in my opinion.

There is much that I don't know about Y2K. All I can do is put together as many pieces of the puzzle that are publicly available and guess what the picture might look like in 2000, even though most pieces remain missing. There is one thing I do know very well, indeed, better than most other investment strategists. Since I've unexpectedly become the Y2K expert on Wall Street, I know the extent to which institutional portfolio managers are taking Y2K seriously.

My sense is that this crowd generally continues to ignore the problem, figuring that it is a known problem, and will therefore get fixed. They've also taken at face value assurances they continue to receive from CEOs of major corporations that they are working on the problem and expect to have it solved in time. However, over the past two months or so, I've been receiving more and more requests from major money managers to visit with them and discuss Y2K with everyone in their shop, even their IT staffs. In other words, Y2K is now on the radar screen of top investors, though their asset allocation and portfolio decisions have yet to be influenced at all by this problem. Interestingly, the IT folks have in no instance so far disagreed with my analysis and predictions.

When I'm asked about asset allocation by the managers of large balanced funds in light of my concerns about Y2K, I recommend a weighting of 10-40-50 in cash, bonds, and stocks. This recommendation recognizes that many managers have to be invested in stocks. Indeed, many equity portfolio managers must be 100% invested in the stock market. The next table shows which industry groups in the stock market should be overweighted or underweighted in preparation for a possible severe Y2K recession.

Playing The End Game. Individual investors are much freer to choose their asset allocation than are most institutional investors. For those of you who believe that Y2K must be reflected in your asset decisions, I offer the two tables below.

I am not advising you to adopt this portfolio strategy right now. Since very few investors are concerned about Y2K at this time, the stock market could still move higher over the next few months. Don't expect a "SELL EVERYTHING" call from me. It's not my style, and I'm not smart enough to pick the top in stock prices. The Y2K asset allocation model below is just one of many possible ones to consider in the event that Y2K becomes a major event in the financial markets. The fact is that no one can make financial and other important decisions for you, in general, and especially in anticipation of the uncertain impact of Y2K on all of our lives.

Yardeni's Equity Portfolio Recommendations for Y2K Scenario

Overweight	Underweight
Consumer	
Food & Drug Stores	Restaurants
Beverages	Department Stores
Tobacco	Autos
Discount Department Stores	Furnishings
Home Improvement	Casinos
Hospitals	
Drugs	
Publishing & Newspapers	
Entertainment	
Financial	
Regional Banks	Money Center Banks
Insurance	Brokers & Investment Managers
Transportation & Shipping	
Trucking Services	Airlines
	Air Freight
	Railroads
Business	
Temporary Personnel	Capital Goods
Security Services	Aerospace/Defense
Utilities	Packaging & Containers
	Basic Materials
	Energy
Technology	
Personal Computers	Semiconductor Equipment
Computer Services	Semiconductor Manufacturers
Networking	Photography/Imaging
Distributors	

* Surgeon General's Warning: Y2K could be very bearish for all stocks. This table is only a guide for possible relative performance in a bear market!

Yardeni's Y2K Financial Asset Allocation Model for Individuals

Cash (currency, multiple deposits, money market, gold coins)	**25%**
Government Securities (1 to 10 year maturities)	**40%**
Equities (US and Europe, blue chip)	**15%**
Speculative Assets (equity puts, zero-coupon bonds, commodity shorts)	**20%**
Risky Assets (emerging markets, real estate investments, commodities)	**0%**

* This is just one of many possible model portfolios. It is based on a 70% chance of a global recession in 2000. No assurances about performance are given.

Appendix I:

Seven-Point Y2K Strategic Plan

1) **Year 2000 Alliance.** The leaders of the Group of Eight (G8) should form a Y2K Global Alliance to coordinate both national and multinational campaigns. The Alliance should be broadened to include all 29 members of the OECD and selected representatives of the United Nations.

2) **Commander-In-Chief.** The Y2K Alliance could use the expertise of military personnel. They should be involved because they have the necessary training and experience for marshaling and mobilizing resources for such a potentially huge global campaign. The G8 should appoint a Y2K Commander-in-Chief.

3) **Military Fail-Safe System.** Military leaders of the United States, other NATO members, and Russia must jointly assess the risk of an accidental nuclear missile launch or a provocative false alarm. They must rapidly develop a fail-safe joint communication and intelligence network to eliminate any such risk. Measures must be taken to thwart terrorists, hackers, and other malevolent opportunists from taking advantage of any Y2K chaos.

4) **Securing Infrastructure.** Y2K "Sector Alliances" should be responsible for the Y2K campaigns in specific global sectors. The top priority must be to secure the supply of electricity worldwide. Other utilities, including water, gas, sanitation, and telecommunications, must also be secured. Contingency plans for rationing utility usage should be prepared. Other key sectors that may require a global "top-down" approach include government revenue collection and debt servicing, welfare payments, farming, manufacturing, mining, transportation, distribution, retailing, banking, and finance. Y2K "Industry Alliances" should have the power to organize and execute a cooperative and collective battle plan among the world's key industries, including, for example, food, drugs, chemicals, energy, security brokerage and exchanges.

5) **Change Freeze.** Governments should freeze all legislative, regulatory, and information technology (IT) changes that might divert resources from the effort to prepare government and business computer systems for the century date change. The Industry Alliances should adopt a similar "change freeze."

6) **Mandatory Y2K Holiday.** The Y2K Alliance should consider requiring all nonessential employees to stay home during the first week of January 2000. Financial markets might have to be closed during this period. This global Y2K holiday would give IT personnel the opportunity to stress test their systems with a slow "reboot," rather than under peak load conditions. They could first test the integrity of basic utility services, especially electricity and telecommunications services. Then they could bring their own systems on-line in a phased sequence that can pinpoint weak links and either repair them quickly or take them immediately "off-line."

7) **Emergency Budget.** The Year 2000 Alliance Accord should require all participants to fund a Y2K Emergency Budget with an initial minimum balance of $100 billion. They should be prepared to provide much more, if necessary. The budget should be spent on both last-ditch efforts to repair or replace key computer systems around the world and to implement contingency plans once the weakest links have been identified. Conceivably, the funds may be needed to purchase strategic stockpiles of fuel, food, and medical supplies.

APPENDIX II

APPENDIX II

HOUSE BILL 2406

⇒ House Bill 2406 currently reads:

Section 8503. Certain computer problems.

Nothing in this chapter shall authorize an action against ***a Commonwealth party*** *or* ***a local agency*** *based on a computer problem related to the additional digits required in some computer programs to distinguish dates in the year 2000 from dates in this century.*

⇒ Section 8501 of Title 42 of the Pennsylvania Consolidated Statutes contains the following definitions:

"Commonwealth party." A Commonwealth agency and any employee thereof, but only with respect to an act within the scope of his office.

"Local agency." A government unit other than the Commonwealth government. The term includes an intermediate unit.

⇒ **Under current Pennsylvania case law, private businesses performing governmental duties are NOT considered a "local agency" and would not therefore be protected under House Bill 2406 in its current form.**

⇒ The definition of a ***local agency*** under Section 8501 of Title 42 of the Pennsylvania Consolidated Statutes should be revised as follows:

"Local agency." A government unit other than the Commonwealth government. The term includes an intermediate unit ***or any entity which is appointed by a government unit other than the Commonwealth government to perform a governmental duty or function, whether ministerial in nature or otherwise.***

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

Session of

NO. 2406 1998

INTRODUCED BY: CALTAGIRONE, BELARDI, READSHAW, HORSEY, M. COHEN, McCALL, GIGLIOTTI, LAUGHLIN AND GANNON, MARCH 12, 1998

REFERRED TO COMMITTEE ON JUDICIARY, MARCH 12, 1998

AN ACT

Amending Title 42 (Judiciary and Judicial Procedure) of the Pennsylvania Consolidated Statutes, providing for sovereign immunity, governmental immunity and official immunity with respect to certain computer problems.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. Title 42 of the Pennsylvania Consolidated Statutes is amended as follows:

Section 8501. Definitions.

"Local agency." A government unit other than the Commonwealth government. The term includes an intermediate unit or <<+ any entity which is appointed by a government unit other than the Commonwealth government to perform a governmental duty or function, whether ministerial in nature or otherwise. +>>

<<+Section 8503. Certain computer problems.

Nothing in this chapter shall authorize an action against a Commonwealth party or a local agency based on a computer problem related to the additional digits required in some computer programs to distinguish dates in the year 2000 from dates in this century.+>>

HOUSE BILL 2273

⇒ House Bill 2273 currently provides:

Section 8531. Immunity for certain erroneous computer information.

> *(a) General rule. – No cause of action, including, but not limited to, any civil action or action for declaratory injunctive relief, may be brought against an* ***immune contractor*** *or* ***an officer or employee of the Commonwealth*** *or* ***any of its agencies or political subdivisions*** *on the basis that a computer or other information system that is owned or operated by any of those persons produced, calculated or generated an incorrect date, regardless of the cause of the error.*
>
> *(b) Contract requirement. – Any contract entered into by or on behalf of and in the capacity of the* ***Commonwealth, an immune contractor or an officer or employee of the Commonwealth or an of its agencies or political subdivisions*** *shall include a provision that provides immunity to those persons for any breach of contract that is caused by an incorrect date being produced, calculated or generated by a computer or other information system that is owned or operated by any of those persons, regardless of the cause of the error.*

⇒ **House Bill 2273, in its current version, does not specifically protect private businesses performing governmental duties or functions.**

⇒ The definition of a ***local agency*** under Section 8501 of Title 42 of the Pennsylvania Consolidated Statutes should be revised as follows:

> *"Local agency." A government unit other than the Commonwealth government. The term includes an intermediate unit* ***or any entity which is appointed by a government unit other than the Commonwealth government to perform a governmental duty or function, whether ministerial in nature or otherwise.***

⇒ New Section 8531 should read:

Section 8531. Immunity for certain erroneous computer information.

(a) General rule. – No cause of action, including, but not limited to, any civil action or action for declaratory injunctive relief, may be brought against an ***immune contractor*** *or* ***an officer or employee of the Commonwealth*** *or* ***any of its agencies or political subdivisions*** ***or a local agency of any political subdivision*** *on the basis that a computer or other information system that is owned or operated by any of those persons produced, calculated or generated an incorrect date, regardless of the cause of the error.*

(b) Contract requirement. – Any contract entered into by or on behalf of and in the capacity of the ***Commonwealth, an immune contractor or an officer or employee of the Commonwealth or an of its agencies or political subdivisions*** ***or a local agency of any political subdivision*** *shall include a provision that provides immunity to those persons for any breach of contract that is caused by an incorrect date being produced, calculated or generated by a computer or other information system that is owned or operated by any of those persons, regardless of the cause of the error.*

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

Session of

NO. 2273 1998

INTRODUCED BY: GANNON, CALTAGIRONE, ALLEN, SEYFERT, ROBINSON, STERN, STABACK, LEH, OLASZ, MASLAND, MCNAUGHTON, GEIST, DALEY AND READSHAW, FEBRUARY 25, 1998

REFERRED TO COMMITTEE ON JUDICIARY, FEBRUARY 25, 1998

AN ACT

Amending Title 42 (Judiciary and Judicial Procedure) of the Pennsylvania Consolidated Statutes, further providing for governmental immunity relating to computer errors.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. Title 42 of the Pennsylvania Consolidated Statutes is amended by adding a heading and a section to read:

Section 8501. Definitions.

"Local agency." A government unit other than the Commonwealth government. The term includes an intermediate unit or <<+ any entity which is appointed by a government unit other than the Commonwealth government to perform a governmental duty or function, whether ministerial in nature or otherwise. +>>

<<+ TECHNOLOGICAL IMMUNITY +>>

<<+ Section 8531. Immunity for certain erroneous computer information. +>>

<<+ (a) General rule. – No cause of action, including, but not limited to, any civil action or action for declaratory injunctive relief, may be brought against an immune contractor or an officer or employee of the Commonwealth or any of its agencies or political subdivisions or any local agency of any political subdivision on the basis that a computer or other information system that is owned or operated by any of those persons produced, calculated or generated an incorrect date, regardless of the cause of the error. +>>

<<+ (b) Contract requirement. – Any contract entered into by or on behalf of and in the capacity of the Commonwealth, an immune contractor or an officer or employee of the Commonwealth or an of its agencies or political subdivisions or any local agency of any political subdivision shall include a provision that provides immunity to those persons for any breach of contract that is caused by an incorrect date being produced, calculated or generated by a computer or other information system that is owned or operated by any of those persons, regardless of the cause of the error. +>>

<<+ (c) Applicability. – Any contract subject to the provisions of this section that is entered into or on or after June 30, 1998, shall be granted the immunity provided for by this section and any provision of a contract which is in conflict with this section is void. +>>

<<+ (d) Expiration. – This section shall expire December 30, 2005. +>>

Section 2. This act shall take effect immediately.