S. HRG. 106–343

Y2K & RUSSIA: WHAT ARE THE POTENTIAL IMPACTS AND FUTURE CONSEQUENCES?

HEARING

BEFORE THE

SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

ON

UNDERSTANDING HOW THESE Y2K POTENTIAL FAILURES, BOTH IN THE SHORT AND LONG TERM, MAY IMPACT ON CURRENT U.S. POLICY INITIATIVES AND WHAT WE CAN DO TO ADDRESS THESE POTENTIAL PROBLEMS WITH RESPECT TO RUSSIA

SEPTEMBER 28, 1999

Printed for the use of the Committee

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

62–345 CC WASHINGTON : 2000

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402

SPECIAL COMMITTEE ON THE
YEAR 2000 TECHNOLOGY PROBLEM

[Created by S. Res. 208, 105th Cong., 2d Sess. (1998)]

ROBERT F. BENNETT, Utah, *Chairman*

JON KYL, Arizona
GORDON SMITH, Oregon
SUSAN M. COLLINS, Maine
TED STEVENS, Alaska, *Ex Officio*

CHRISTOPHER J. DODD, Connecticut,
Vice Chairman
JOHN EDWARDS, North Carolina
DANIEL PATRICK MOYNIHAN, New York
ROBERT C. BYRD, West Virginia, *Ex Officio*

ROBERT CRESANTI, *Staff Director*
T.M. (WILKE) GREEN, *Minority Staff Director*

CONTENTS

STATEMENT BY COMMITTEE MEMBERS

CHRONOLOGICAL ORDER OF WITNESSES

ALPHABETICAL LISTING AND MATERIAL SUBMITTED

Y2K & RUSSIA: WHAT ARE THE POTENTIAL IMPACTS AND FUTURE CONSEQUENCES?

TUESDAY, SEPTEMBER 28, 1999

U.S. SENATE,
SPECIAL COMMITTEE ON THE YEAR 2000
TECHNOLOGY PROBLEM,
Washington, DC.

The committee met, pursuant to notice, at 10:02 a.m., in room SD–192, Dirksen Senate Office Building, Hon. Christopher J. Dodd (vice chairman of the committee), presiding.

Present: Senators Bennett, Dodd, and Lugar.

OPENING STATEMENT OF HON. ROBERT F. BENNETT, A U.S. SENATOR FROM UTAH, CHAIRMAN, SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM

Chairman BENNETT. The committee will come to order. We appreciate your being here this morning. Senator Dodd, the vice chairman of the committee, will be chairing the hearing, and he is on his way. Prior to his arrival, I would like to make a comment or two about the subject of today's hearing.

A serious social, economic, and political crisis began when Russia devalued the ruble and then defaulted on its debts. That was in August 1998. Little work has been done to investigate the long-term consequences that Y2K would bring to a Russia already on the edge. That, of course, troubles this committee since Y2K failures in key infrastructures such as power, banking, telecommunications, and defense could have some serious negative impacts on the stability of the Russian economy and on their political environment which already is wrought with enough problems.

The international monetary fund announced last Friday that it would offer special loans to countries suffering serious economic damage from Y2K. The IMF certainly hopes that this financial assistance won't be needed, but they say in their statement: "There are uncertainties, and the potential consequences for international trade and growth of possible interruptions to production and shipment may be significant." I think these uncertainties and potential consequences resulting from Y2K apply to Russia as much as they do to any nation.

Now, Russia is not as highly networked and interconnected as is the United States, but it still relies on information systems and microchips. In fact, the information systems that survived the Soviet Era and remain in use are extremely critical. As many as 4,000 Soviet-era mainframes are estimated to support the operation of Russia's industrial and defense enterprises. It is believed

that several hundred million dollars would be needed to repair these systems.

The failure, disruption or corruption of these systems in a short span of time could create a unique and unexpected challenge to the economy. In the short term, the shock from serious Y2K failures could exacerbate Russia's downward economic spiral. Since such an event would unquestionably affect U.S. policy, we must proactively consider how we should respond to these failures if and when they should occur.

From a long-term perspective, no one knows what the impact of Y2K inefficiencies will mean for the Russian economy as a whole. We must decide soon what our foreign policy will be with respect to Y2K failures. We cannot engage in diplomatic shell games until November 1999 and then glibly announce the U.S. foreign policy on Y2K. What is more, I fear that whatever policy the White House has arrived at may crumble when the first CNN footage hits the air, because very often the CNN footage determines the policy.

What should U.S. policy be with respect to foreign Y2K failures? How will we prioritize national security, the needs of our allies, the needs of critical trading partners, and of course humanitarian needs? These will be very difficult decisions, and there will be no time for "spinning" decisions. Different decisions will demand prompt and careful attention.

The U.S. does not have the resources to save the world. Indeed, if it weren't for the rapid actions of a member of this committee, Senator Stevens, who happens to double as the chairman of the Appropriations Committee, we would not have had the emergency funds to meet emergency requirements here at home.

It is vital to remember that Y2K problems unfold over time. They do not all occur on January 1st. We, here in Washington, have expended a lot of effort to examine the immediate impact of Y2K, from sharing nuclear information to collecting information about telecommunications. However, we have given little consideration to what happens if and when problems emerge in late January or in March, and as our recent report makes clear, we expect the majority of those problems to emerge overseas.

Now, since the dissolution of the Soviet Union, America has reached out to try to help the Russian Federation wherever it was prudent to do so. We are most fortunate to have one of the Senate's foremost Russian experts and a valuable member of the committee, who normally sits up here with us and today is sitting there, as our first witness.

In 1991, Senator Lugar recognized the urgent need to help Russia move its nuclear and chemical weapons back within its sovereign borders. So he has been an early warning system, if you will, on these problems and what needs to be done to prepare ourselves and protect ourselves.

Through Cooperative Threat Reduction, the U.S. and Russia collaborated to dismantle launchers and destroy chemical weapons in the newly independent states. It is precisely because of this expertise that we have invited him here today to share his thoughts about how assisting the Russians with Y2K fits into the broad goals of threat reduction.

My only regret about this hearing is that I will be unable to stay for most of it. This hearing comes as a result of the initiative and energy of Senator Dodd who has on the committee provided the leadership to focus on these very problems. So Senator Dodd, the vice chairman of the committee, will chair this hearing today. I will do my best to get back as often as I can and stay as long as I can.

Senator Dodd, the gavel and the hearing are now yours. I have said all I know about this.

[The prepared statement of Chairman Bennett can be found in the appendix.]

OPENING STATEMENT OF HON. CHRISTOPHER J. DODD, A U.S. SENATOR FROM CONNECTICUT, VICE CHAIRMAN, SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM

Vice Chairman DODD. Well, thank you very much, Mr. Chairman, and I appreciate the gavel. My only regret is this committee does not have legislative authority. But I thank you very, very much, Mr. Chairman, and let me join you in welcoming our colleague on this committee, and also the Senate, who we will hear from shortly on this issue. And he does bring, as you pointed out, a tremendous amount of expertise and has devoted a good part of his Senate career in the latter years, particularly on the Russian issue, working with Sam Nunn, our former colleague, on a number of proposals that I think have made a difference already, maybe not that have lived up to even his expectations of what we might accomplish, but without them, I think we would have been in a lot worse shape today.

And while there is much to be concerned about within Russia, there is good news there too. We have a tendency to focus on all that is wrong, and there are a lot of problems, but today we hope to focus, if we can, on some of the critical Y2K issues, and certainly it is not the chairman's intention nor mine to engage in any beating up on Russia or embarrassing them. Quite to the contrary.

Russia is now emerging as an important ally. We have a lot of common interests we need to work on together, and we need to find out ways in which we can be helpful in a positive and constructive way. So I am particularly anxious to hear what my colleague from Indiana has to say.

And let me just share, if I can, a few thoughts of my own on this subject matter. The goal of the hearing, if I may say so, is to try to understand how these Y2K potential failures, both in the short and long term, may impact on current U.S. policy initiatives and what we can do to address these potential problems with respect to Russia.

Home to almost 150 million people, Russia spans 12 time zones. It is the thirtieth largest trading partner of the United States. There is some 11,000 of our fellow citizens who live in Russia. Certainly, it is not the largest trading partner nor the biggest host to U.S. citizens, but we all recognize that Russia continues to be an important U.S. foreign policy concern for more than 50 years.

Since the end of the cold war, U.S. policy goals with respect to Russia have broadly fallen into two categories: reducing the threat of nuclear weapons, and supporting Russia's efforts to transform its

political and economic system. Both of these, I would stress, are long-term goals that admittedly will take years to achieve.

Russians struggle with many difficult issues including the 80 percent devaluation of the ruble in 1998. The government and financial instability has spurred capital flight of $1 billion a month to leave Russia. In the past year alone, Russia has lost some $15 billion in capital to foreign banks.

Now, the country must, in the midst of all of this and there are many issues, confront the Y2K challenge. In March, the Department of State testified that the U.S. would need, and I quote them, "a robust policy framework in order to prioritize responses to international Y2K failures". I am interested to learn today what this policy framework will be with respect to Russia.

Many policy experts have viewed Y2K as a short-term problem, one best left to "techies" and not likely to impact enduring policy concerns. Unfortunately, according to the Gartner Group, many Y2K problems will only emerge in the weeks and months beyond January 1, 2000, as the chairman just alluded to.

Today the committee seeks to better understand Russia's highly unique situation and whether Y2K could erode stability that we take for granted in our ongoing bilateral initiatives. Before I go any further, I want to specify what I mean by long-term Y2K concerns. Many organizations responsible for key Russian infrastructures lack the financial resources to make the necessary fixes. For example, Rostelecom, Russia's long distance and international carrier, is reportedly unable to upgrade its seven gateway switches and is choosing to implement, and I quote, "workarounds". Meanwhile, regional carriers have only just begun testing their networks.

Lack of funding will force many to create their own ad hoc fixes, and while these "workarounds" are likely to prevent immediate failures and keep connectivity, they could degrade capacity. In short, Russia could lose communications capacity, stability, and profitability. In fact, you will hear testimony today about the fact that six out of seven direct communication links from Moscow to Washington that are used in times of crisis would experience—would experience—Y2K failures. Let me emphasize: That is six out of seven key national security links could fail and will fail if the fixes are not implemented.

These critical links will be fixed, we are told, but what about the bulk of commercial communications? The United States has to carefully consider the impact of Russian infrastructure failures in our relations with them.

Today we will also consider the concerns of the Department of Defense and State, along with Energy. On September 13th, the Department of Defense and the Russian Ministry of Defense signed an agreement indicating their intent to establish the Center for Year 2000 Strategic Stability during the year 2000 transition period, a subject we have discussed many times in this committee. In this center, U.S. and Russian military personnel will sit side by side and continuously monitor U.S.-provided missile and space launches information. I would like to remind the audience that Russia still has approximately 6,000 strategic nuclear weapons and over 1,000 delivery systems.

The center will also provide an important link to communicate other defense-related events that could be potentially destabilizing such as an aircraft going off course due to navigation or communication system Y2K failure. Last week, nine military officials from Russia were in Colorado to discuss the details of this proposal, and I am very optimistic and heartened by this turn of events in the last few weeks.

Also last week, the Congress passed the Defense Authorization Bill. It is now waiting to be signed into law, which may happen, in fact, even today or tomorrow or the next day. This bill provides for over $475 million for Cooperative Threat Reduction programs. In August, the Russian Ministry of Defense requested $15 million to address Y2K-related security risks for the control and protection of weapons-grade nuclear materials. This bill requires Russia be recertified by the administration. I am told that will be a part of this effort and part of this bill. So that is good news. Unfortunately, it can take several months, but we hope that we won't lose any time in this matter.

Reliable energy is of key importance to the entire nation. In August, with unified energy systems, the Russian electrical monopoly cut power to some 20,000 customers just to save fuel for the winter. What this means is that fuel reserves for Russia's electrical power monopoly will be as low as the country heads into Y2K. The Department of Energy is working closely with Russia as it develops the necessary contingency plans that will be needed to maintain grid stability.

Nuclear power plants are a serious concern for Russia. Russia has 29 nuclear power reactor units in operation at 9 different sites. Western-style nuclear power plants employ an uncompromising set of in-depth safety elements, including a massive reinforced concrete structure called the containment facility, to prevent the release of radioactivity. Most Soviet-designed reactors do not have such a containment structure. The most infamous plant without a containment structure is the Chernobyl-style reactor, and there are 11 of these reactors at three locations in Russia.

While these plants do not have direct Y2K vulnerabilities, they can only withstand a loss of power for approximately 90 to 120 minutes before they begin to have core damage. In a country where disruptions of power supply are common before Y2K, special consideration needs to be paid to the months and years beyond Y2K to reduce the chances that sudden power loss could compromise the power plant safety.

Primary plant safety systems are on the front line of defense against accidents, and no Y2K issues have been found here. However, other systems important to safety and plant operations are of concern, such as plant process computer and information display systems. A Y2K-related malfunction in these systems would complicate operations and increase the chances of operator error. Operator error, as we all know, ultimately led to the Chernobyl accident. The combination of human error and computer error is one of the greatest Y2K challenges for Russia and the rest of the world.

So with those initial thoughts, again I want to thank the chairman for holding the hearing, for his untiring efforts on these issues, but particularly this one as well, and to thank our witnesses

in advance for their participation today and to particularly thank you, our colleague from Indiana, for his presence here this morning, and Senator Lugar, we are anxious to hear your thoughts.

[The prepared statement of Vice Chairman Dodd can be found in the appendix.]

STATEMENT OF HON. RICHARD LUGAR, A U.S. SENATOR FROM INDIANA

Senator LUGAR. Thank you very much, Mr. Chairman. It is a privilege to be with you today. I want to talk about U.S.-Russian cooperative activities in response to the Y2K computer problem.

Since the end of the cold war, I have taken a great deal of interest in U.S. policy toward the former Soviet Union. As the Soviet Union began to break apart in 1991, Russian leaders came to former Senator Nunn of Georgia and me and pointed out the dangers of the dissolution of a nuclear superpower.

The viability of the entire Soviet weapons custodial system was in doubt. There were tons of weapons and materials of mass destruction spread across hundreds of sites in Russia and other former Soviet states. Russia requested our cooperation in securing and dismantling its nuclear arsenal and weapons-usable materials, and this was the genesis of the Nunn-Lugar Cooperative Threat Reduction Program.

This was not a problem that Congress wanted to deal with in 1991. The atmosphere was decidedly against any initiative that focused on a foreign problem. Americans were tired from the cold war and the Gulf War, and yet we brought together a nucleus of Senators who saw the problem as we did. The Nunn-Lugar program was passed in the Senate by a vote of 86 to 8 and went on to gain approval in the House and was signed into law by President Bush.

While much remains to be done, the Nunn-Lugar scorecard is impressive. It has facilitated the destruction of 365 ballistic missiles, 343 ballistic missile launchers, 49 bombers, 136 submarine missile launchers, 30 submarine-launched ballistic missiles. It has sealed 191 nuclear test tunnels, and, most notably, 4,838 warheads that were on strategic systems aimed at the United States have been deactivated, all at the cost of less than one-third of a percent of the Department of Defense's annual budget.

Without Nunn-Lugar, Ukraine, Kazakstan, and Belarus would still have thousands of nuclear weapons. Instead, all three countries are nuclear weapons-free.

I offer this as a useful example to cope with another problem that has arisen in our post-cold war relationship, namely the impact of Y2K. The atmosphere surrounding the current Russian-American relationship and its implications for our national security are not unlike those that existed in 1991. I believe that it is in the United States' national security interest to again cooperate with the former Soviet Union to reduce the threats our country may face.

Mr. Chairman, we do not know what is going to happen to Russian computer systems when we pass into the millennium, and neither do they, but initial estimates do not appear to be promising. In May, the American Chamber of Commerce in Russia pointed to

a study that paints a disturbing picture of the impact of Y2K in Russia, and I quote: "Utilities will operate at 40 percent of capacity for the first 2 months of the year 2000. Transportation will be disrupted 80 percent of the time and telecommunications 50 percent of the time for a 3-month period. Hospitals will be forced to treat only emergencies for at least 2 months. Financial markets will be disrupted for 30 trading days, and banks will be disrupted for 20 business days." Obviously, these estimates are disturbing and beg the question of whether similar problems will affect the Russian military and strategic forces.

I am not going to push the panic button. In my visits to Russia and in briefings and conversations with experts on these subjects, I have been convinced that the chances of an accidental missile launch as a result of a Y2K problem are almost nonexistent, but Y2K may cause other problems in Russian strategic systems.

It is in our interest to take out a kind of insurance policy to ensure that the transition to the new millennium does not exacerbate the situation. Cooperative activities and programs that reduce these threats are in our national security interest, that of the United States and that of Russia, provided they are implemented in a responsible manner.

Experts agree that cooperation over the transition period needs to center on three specific areas: early warning systems, nuclear weapon security, and nuclear power plants.

Our Department of Defense began discussing the potential impact of Y2K with Russian counterparts in June 1998. These efforts culminated in an agreement to establish a Center for Y2K Strategic Stability in Colorado Springs, Colorado. The center will ensure that for the last few weeks of December 1999 and the first weeks of January of the year 2000, U.S. and Russian military officers will sit side by side and monitor early warning data generated by satellites observing missile activity around the world to ensure that potential mishaps caused by Y2K do not lead to strategic miscalculations and mistakes.

Mr. Chairman, it is in the interest of the United States to ensure that Russia understands the kinds of problems they may encounter with strategic systems so that there are no surprises or confusion on January 1. We want them to understand that their problems are Y2K-related and not a result of U.S. hostile action for which they need to respond. This requires consultation, awareness of potential Y2K failures, and training of key personnel, and this kind of cooperation is clearly of as much value to the United States as it is to the Russians.

Russian early warning operators may not be able to tell the difference between a peaceful rocket and a military rocket from their computer screens. Russian early warning capabilities continue to deteriorate, and this deterioration will be compounded by the transition to the year 2000. Russian Major General Dvorkin recently suggested that the Y2K problem could lead to incorrect information being transmitted, received, displayed, or complete early warning system failures. We should heed those concerns.

I am sure we remember the convulsions the Russian command and control system endured several years ago when a peaceful Nor-

wegian rocket launch activated President Yeltsin's nuclear briefcase. Fortunately, the Russians realized their mistake.

The center in Colorado is meant to create an atmosphere for both sides to work together to resolve any missile launch detection, false alarms, or other ambiguities that may arise. I am hopeful the Russian military officers serving on the second floor building of 1840 at Peterson Air Force Base will, in the event of a Russian malfunction, be able to provide Moscow with the accurate information and data necessary to eliminate misperceptions.

The continuous safe and secure storage of the Russian nuclear stockpile is the second area that will be complicated by Y2K. Over the last six or 7 months, the Department of Defense has sought to engage its Russian counterparts on the nuclear warhead protection, control, and accounting systems. Early in the discussions, the Russian Ministry of Defense admitted it had not considered the impact Y2K could have on their systems. The need for U.S. assistance in the area is clear. As members of the Senate, we have had countless briefings on the groups of individuals attempting to illicitly acquire these weapons.

More recently, the Russians have made substantial progress in acknowledging and responding to these potential problems. The Russian Ministry of Defense is committed to establishing and maintaining special Y2K monitoring stations at their largest warhead storage facilities. Stations will be manned 24 hours a day by officers specially trained to monitor physical security, environmental controls within the facility, telecommunications, and power levels. These efforts and establishments mark a tremendous improvement.

At Pentagon urging, the Russian have conducted capability assessments to gauge their ability to respond to an emergency. Unfortunately, the results of the assessments were not encouraging. Due to the lack of appropriate response equipment, it is clear there are significant deficiencies in their capabilities to respond to intrusions and other potential threats. Our Defense Department is seeking to assist Russia in these efforts through other Nunn-Lugar programs.

The Russian Ministry of Defense has requested approximately $15 million in equipment to upgrade their ability to respond to an emergency. I understand that Assistant Secretary of Defense Warner will testify later, so I will not attempt to describe the details of that assistance, but I have been told that the Pentagon has reviewed the request and has determined it to be reasonable and consistent with the Nunn-Lugar conditions and restrictions.

Mr. Chairman, the Pentagon reports that a portion of the request can be fulfilled immediately using prior year Nunn-Lugar monies. However, the remainder of the Y2K assistance must await a recertification requirement in the Fiscal Year 2000 Defense Authorization Conference Report. The executive branch is hopeful the process will be completed on or around October 1.

Mr. Chairman, this committee must watch the situation closely. I believe the delivery of this assistance to be in United States' interests. Delays and the recertification process might possibly slow Y2K assistance to the point where the equipment arrives after the first of the new year. The Senate must view this additional and redundant recertification as a self-inflicted wound that must not be

permitted to interfere with important national security goals. This committee, the Senate Armed Services Committee, and the Committee on Appropriations must be prepared to expunge such duplicative requirements should American interests dictate.

Mr. Chairman, I have learned this morning, and you related that there is optimism that the recertification certificates can be signed, that it can be a part of the Presidential signature of the Authorization Bill, and we hope and pray that that will occur as promptly as possible.

The potential threats emanating from Y2K problems in Soviet-designed nuclear reactors is a third area of concern. Historically, safety mechanisms and procedures at these reactors are poor. The reactors suffer from deficiencies in design, operator training, and safety procedures. Reactor operations and support staff face low and erratic pay, training shortfalls, and deficiencies in safety procedures.

Unfortunately, these problems are compounded by a very late start in preparing for the transition to the new millennium by the states of the former union and central and eastern Europe. Although neither a melt down or a failure of primary safety systems is likely, it is in our interests to continue to work to prevent these potential threats.

Many believe that Soviet-designed reactors are immune to Y2K-generated problems because they utilize older analog systems, but this is incorrect. Digital overlays were installed to improve performance, monitoring, and safety response and are susceptible to Y2K problems. If these systems were to malfunction, operators could be blind to some reactor functions or receive erroneous data that could lead to improper actions. In U.S. reactors, this would not pose a problem because of built-in redundancy of our systems. Unfortunately, redundancy is not present in most Soviet-designed plants.

Reviews of Soviet-designed reactor susceptibility to Y2K-induced problems revealed that host countries lacked the resources to conduct threat evaluations, and significant safety issues were at stake. Officials of the Department of Energy worked closely with their counterparts to develop assessment guidelines in order to determine potential problems that might arise during the millennium transition.

U.S. expert assistance was crucial in overturning initial complacency expressed by these nations. The Department of Energy played an important role in completing the detailed risk assessments of the various Soviet-designed reactors and providing assistance to begin remediation of hardware and software problems. It is clear that without the Department of Energy's efforts, the risks of an accident would have been much higher.

Given the existing timeframe, it is too late to fix every Russian system. Our efforts must continue to concentrate on reactor safety systems, contingency planning, and engagement with the Russian Ministry of Atomic Energy on these subjects. Transparency and consultation in these areas are in U.S. interests. Furthermore, I believe our country must make every effort to warn Americans abroad, living or working near these reactors, of the problems they may face as a result of Y2K.

One of my personal concerns is the impact of local and Federal Government pressure to keep Soviet design reactors on line in the face of strain and uncertainty. It will be the dead of winter with temperatures propping far below freezing. Local and state Governors and mayors in Russia, as well as officials in national capitals, will be loathe to permit nuclear reactors to shut down. Political pressure, in addition to monitoring failures and the loss of offsite power, may contribute to failures in judgment which could lead to accidents.

Recently, Russian Atomic Energy Minister Adamov reported to a conference in London that he believed that Russia had achieved "the same level of safety as western units, end of quote". He went to explain that the rate of unplanned shutdown at Russian reactors were equal to that of Germany and lower than France and the United States. I am hopeful his confidence is borne out, but it is in our interest to continue to cooperate in alleviating the problems inherent in the 65 nuclear reactors at 20 sites in 9 countries of the former Warsaw Pact and former Soviet Union. If not handled properly, these reactors could prove threatening to American interests. We must not forget that one of these sites is less than 130 miles from Alaska.

Mr. Chairman, I began my testimony with the recommendation that we view efforts to eliminate potential threats to U.S. security from Y2K-generated problems in Russia as an insurance policy. In my opinion, an insurance policy in this area is a good investment. The cost of efforts to address potential threats today will be minuscule in comparison to the cost of responding to future tragedy should an accident occur.

I understand that the atmosphere today may not be all that conducive to engagement and cooperation with Russia. Congressional committees are investigating allegations of corruption of Russian government officials. As I indicated in my introduction, the Senate has faced similar circumstances before, and there are many parallels between the mood today and that which Senator Nunn and I faced in 1991, but I would encourage my colleagues to once again look to the future and to examine the benefits of cooperating with Russia on Y2K versus the potential costs of inaction.

In 1991, the Senate courageously supported the Nunn-Lugar program in the face of widespread discontent with foreign affairs. That investment has paid tremendous dividends in our national security. I would urge this committee and the Congress to once again provide our country with the leadership necessary to protect that national security. I am not suggesting a blank check for Moscow, but our government must again engage the Russian people through the auspices of the Department of Defense and Energy and our private sector. Strict management and accountability of cooperative efforts with Russia will protect our investments. We have made important progress. It is clear there is much work to be done.

I praise your foresight and that of the chairman in examining these issues, and I look forward to working with you as a member of the committee on the threats facing our country.

Vice Chairman DODD. Thank you very, very much, Senator Lugar. That is excellent testimony, and I just want to pick up on your last comments. I think it is very, very important, and this is

not—we are not talking about a blank check here, obviously. That would be unacceptable, but the important notion of staying engaged here during this critical period, even if the Y2K issue were not an issue here, I would make the same case, as I am sure you would.

But this does give us an opportunity to reconnect in a way, because I think so much of what we hear of our country deciding we're going to disengage or spend our time investigating what is going on in Russia, while it has legitimacy to it, if that is the only news that is coming out of Washington, then I think it is going to be harder to build those necessary bridges that are going to be essential for the kind of cooperation on a whole host of other areas. And while Y2K poses some serious problems, as you have pointed out, it also creates some significant opportunities.

So I am hopeful in light of what we have heard now, by the way of the signing of the DOD Authorization Bill, that the recertification package can go forward, and we don't have to wait these necessary weeks and months, I think is positive news and will allow us to provide some necessary assistance.

I just wonder if you might comment on the progress of Nunn-Lugar with regard to the 6,000 warheads, the 1,000 launch systems that still exist. What prospects do we have of continuing to reduce these kinds of numbers, in your view, in the coming months and years?

Senator LUGAR. I think the prospects are substantially in our favor on both sides. Clearly, the Senate has been discouraged because we ratified Star II some time ago. Duma has not done so, despite numerous delegations approaching our colleagues in Russia and elsewhere. At the same time, as the chairman is aware, delegations of distinguished Russian military officers have come to this country, and many of us have visited with them, discussing what they see as a potential outline for a Star III treaty or a Star IV or something beyond.

Sometimes radical ideas are given of reduction of warheads to 2,000, each level, or maybe 1,500, or some suggesting even 1,000 as opposed to the 3,500 level more or less that Star II contemplated. As a practical matter, both sides are reducing their weapons because of obsolescence factors, and one of the factors for the nuclear weapons—as well as the Y2K steps that we are talking about accidents, accidents that could envelope citizens in the homeland, and as time goes on the problems of maintenance are more and more acute. So this is leading in a practical way to constructive destruction of these situations. Hopefully, it will be the proper framework the Star regime has given, because that gives assurance to both sides and some degree of verification that is more satisfying than an ad hoc reduction sort of outside that framework.

Vice Chairman DODD. I wonder if you might—I wish I could tell you this was an original idea I had had, but so often Senator Moynihan proposes suggestions and ideas that are a bit ahead of their time, and when this proposal dealing with the Colorado Springs facility first surfaced, he made the casual comment that it might not be a bad idea to examine the possibility—obviously, you want to set up this framework first, but the possibility of having a permanent facility beyond the Y2K issue.

And I wonder if you might just give your own thoughts on that prospect, realizing of course, one step at a time, we have got an initial problem we have the deal with. But do you think, one, it is a good idea? Two, what do you think the possibilities are that we might be able to establish such a permanent facility?

Senator LUGAR. I think the possibilities are excellent. It depends very largely upon Russian cooperation. The Cooperative Threat Reduction programs we are talking about are a very substantial intrusion into Russian space and into Russian planning. Often Americans ask why are Americans involved in destroying Russian missiles, warheads containing Russian material, and the good answer is obviously that Russia understands the potential proliferation for accidents, for maintenance problems. Without the money, without the resources in their defense budget to do these things they would not be done, or they would be done poorly with very great risk to the Russians and the world.

Now, this has meant that even in the ups and downs of the Russian political relationship, the Cooperative Threat Reduction program has flowed on annually because both sides realize this is really crucial. It is not that the politics of the country are inessential, but when it comes down to it, human life, large portions of the country are at stake. So this leads, it seems to me, toward more and more cooperative watching of what we are all doing, the building of confidence in this situation, and it is something that I think we ought to foster.

I agree. The Colorado Springs situation, this may be a blessing of Y2K that has brought us together in this very constructive maneuver there.

Vice Chairman DODD. There are obviously significant differences when expending potential membership in these cooperative efforts, but clearly, although China deals with its nuclear weapons in a very different way than Russia does, Pakistan and India come to mind immediately as potentially other nations that we could draw into Cooperative Threat Reduction efforts, and I wonder if you might just share thoughts on whether or not does that complicate the primary task of dealing with United States and Russia's relationship in this area? It is premature to be talking about that?

Senator LUGAR. No. I don't think it is premature. It requires cooperation. To take the case of India and Pakistan, invitations on their parts for us to be a part of their situation, those invitations have not been forthcoming, but nevertheless, they might be given the right circumstances. I suspect, too, the Russians are interested in a cooperative effort with the United States vis-a-vis other situations, and our agenda in Russia is with treaties we have already ratified such as a chemical weapons convention in which the Russians have ratified this.

We all have testified. There are 40,000 metric tons of chemicals at seven locations. They are fairly well defined, and we believe fairly secure given cooperative work, but almost none of those chemicals are being destroyed in Russia. The budgetary resources simply are not there. So, once again, we are going to have to make some judgments. It is not a question of intrusion on Russian space but as a practical matter.

Is it dangerous or not for 40,000 metric tons to continue, even as we here in this country for our own protection wrestling with this destruction of the chemical weapon stock?

Vice Chairman DODD. And, as you point out, of course the first nation to suffer with deterioration was Russia itself.

Senator LUGAR. Yes.

Vice Chairman DODD. We could probably just spend the day just on these issues alone, and obviously we have got a Y2K issue to look at. So, again, I thank you for your testimony. It has been very, very helpful, and your continuing efforts in this regard, you are really recognized by both sides of the aisle, as we say, Democrats and Republicans, as truly the leader in the Senate on these issues, and we respect your judgment and thoughts immensely.

So you are more than welcome to join us up here. You may have a busy schedule, but I hope you will spend some time with us.

Senator LUGAR. Thank you.

Vice Chairman DODD. Thank you very much.

[The prepared statement of Senator Lugar can be found in the appendix.]

Vice Chairman DODD. And now we will go immediately to our next panel. Panel II consists of three agencies dealing with Russia. Our witnesses include—and I will ask them to join us—John Beyrle—did I pronounce that correctly?

Mr. BEYRLE. That is right, Senator. Thank you.

Vice Chairman DODD. John, we welcome you. John is the Deputy for the Ambassador at Large and Special Advisor to the Secretary of State for Russia and the newly independent states. We thank you for being with us.

The Honorable Edward Warner, III is the Assistant Secretary for Strategy and Threat Reduction at the Department of Defense, and we thank you for joining us.

And Ken Baker is the Principal Deputy Assistant Secretary for International and National Security at the Department of Energy, and, Mr. Baker, we thank you for joining us as well.

Why don't I ask you to begin in the order that I have introduced you, if that is appropriate. And I have got this annoying clock up here, but you have all testified on numerous occasions, and you will appreciate that Senator Lugar and I would urge you to try to get these reports down as tight as you can, but I will leave the clock on only as sort of a trigger in your own mind. I know I have used it periodically as sort of where we are here.

What do we have that clock set to? Seven minutes. Why don't we do it at seven, but don't feel obligated. If you need to go on a few more minutes, don't stop, but that might be of some help.

Again, I thank all of you for your continuing cooperation, and we are very interested to hear what you have to say this morning about where things stand as we are at 94 days, 23 hours, 50 minutes, and 24 seconds.

Mr. Beyrle, your testimony.

STATEMENT OF JOHN BEYRLE, DEPUTY FOR THE AMBASSADOR AT LARGE AND SPECIAL ADVISOR TO THE SECRETARY, THE DEPARTMENT OF STATE

Mr. BEYRLE. Thank you very much, Mr. Chairman. I would like to say it is a real honor to follow Senator Lugar on this panel. As one who has spent much of his adult life thinking about and dealing with problems of the Soviet Union and Russia, I have tremendous respect and admiration. I have to say that, Senator Lugar, what you have done has been a real inspiration of many of us in government. So it is an honor to follow you, sir.

I am pleased to have the opportunity to discuss the potential impacts and the consequences for the Russian Federation of the year 2000 computer problem here. I have a longer statement, Mr. Chairman, which I will ask be entered into the record, and I will summarize it here in the interest of the time.

I think that the fact that focus of this hearing is solely on Russia and Y2K is evidence of the justifiable concern of the Congress and the American people on just how the potential for disruption associated with this change over to the millennium might affect our national security. Now, the two areas that pose probably the greatest potential risk to our national security are those being nuclear weapons and related questions, and nuclear power will be addressed by my colleagues from the Departments of Defense and Energy.

For my part this morning, I would like to open our discussion by providing a brief overview from the perspective of the State Department of our current assessment of some of Russia's Y2K preparations. I would like to emphasize at the outset that our assessment of Russia's vulnerability to Y2K is an ongoing iterative process. We have been and remain continually engaged with Russia, the Russian Government, in an effort to gather the information we need to make a definitive assessment in the areas of greatest concern or those that have the most direct impact on American interests.

In general, the amount and the quality of information available has not been optimal, but it has been sufficient for us to make some evaluative judgments in these key areas, and these are judgments that we are continually reassessing or refining as the situation on the ground changes or as new data become available. But the year 2000 technology problem is, as this committee well knows, without precedent in history and uncertainty shadows all of our efforts to deal with it.

With regard to Russia, especially the challenge lies in assessing how this uncertainty translates into risk. We don't underestimate the potential disruptions that Y2K may bring to Russia, but at the same time we need to evaluate such problems realistically. Russia's success in navigating the Y2K transition throughout its society rests in large part on its ability to minimize its electricity and communications disruptions, and thus I would like to concentrate this brief overview on our analysis of the electrical and telecommunications sectors.

Russia is likely to experience disruptions in its electrical grid and telecommunications infrastructure with subsequent effects on its financial, industrial, and government sectors. At this time, we do not foresee severe long-term disruptions. Our analysis of Russia's elec-

tricity sector indicates the larger cities, Moscow in particular, are likely to be much less affected by outages than will be the countryside. We attribute this partially to the Russian government's traditional concern and attention to urban populations which dates back many decades, as you know. In fact, as we understand the electrical sector priorities, power to the countryside might be reduced temporarily in order to ensure that the cities are not deprived. If the overall integrated power system is not fully functional, this could result in power deficits, perhaps lasting several days to smaller towns and villages.

The power utility's ability to supply electricity will likely vary from region to region. For example, the far east will likely face the greatest risk of power loss or shortages. On the other hand, because of the economic contraction of the past decade, many areas are currently using much less power than previously was the case, and when combined with the extended holiday period which decreases electricity demand, this should result in some excess generation capacity. In turn, this should reduce the stress on the electrical grid and provide a bit more flexibility to the power generation and distribution operators to work around the problems that may develop in individual plants.

It is not secret that Russian winters are cold. Most of us have spent time in them. Any disruption of the heating systems in Russia thus could have serious and potentially life threaten consequences. The reliability of the heating systems is tied closely to the availability of electricity.

In larger cities such as Moscow, heat is provided mostly by natural gas-operated heating plants. Coal-fired plants are more common in the small cities and towns. These plants are analog and shouldn't be affected by Y2K, but once again, electricity is required to run the pumps that pump the water through and return it.

A somewhat greater potential for disruption, in our view, lies with the Russian telecommunications sector. There are two to three thousand domestic telephone companies around the country, and they use a wide variety of equipment produced both domestically and abroad. We believe that some of that equipment contains embedded microprocessors that aren't Y2K compliant. The consequences of this are that some of the systems will likely fail, disrupting normal telecommunication services, and it could take the telecommunication companies days, maybe even weeks, to track down and repair all the failures.

Russia has access to updated telecommunication satellites which we believe to be Y2K compliant. Less clear, however, is the status of the ground-based links, some of which may rely on embedded chips. The government and telecom providers are working to minimize disruptions, but we doubt that they have sufficient time or resources to resolve all the problems in time.

Many vital industries and government entities have one or more backup communications systems. We believe, for example, the Soviet-era internal phone system that connects many government ministries and the Kremlin should continue to function. The electricity monopoly UES has its own communications system using power lines as well as other backup systems, and key energy players like Gazprom, for example, also have doubly redundant

backups which should provide some measure of security in these key sectors.

Given the efforts that Russia has made in remediating potential Y2K disruptions and in making contingency plans, at this time we are hopeful that we will not need to reduce staff in our embassy and three consulates in Russia. We expect to make a final determination on this in mid-October. Nonetheless, we are advising U.S. citizens who will be in Russia over the millennial transition to be prepared for possible disruptions, especially in key sectors like electricity, heat, and telecommunications. And as always, we strongly urge all U.S. citizens to register at one of our missions and remain in contact for updated information.

The U.S. has worked closely with key sectors in Russia to prepare for transition. We focus particularly on those areas related to national security, as my colleagues will relate. In addition, however, thanks to funds appropriated by Congress, we have carried out a number of activities with and inside of Russia. Beginning earlier this year, we cooperated with the Russian Government, the World Bank, and the International Energy Agency, and the American Chamber of Commerce in Russia to conduct a series of workshops and seminars in Russia on the Y2K issue. We have sent U.S. experts to Russia, and we funded the travel of Russian experts to various international meetings and conferences.

USIA has also developed a Russian language web site on Y2K to provide basic public information about the problem. However, a recent poll indicated that only 50 percent of Russians surveyed had even heard of Y2K. I think that compares with something like 70 to 80 percent in our own country. So clearly the Russian Government still has a way to go in bringing the reality of Y2K to its own citizens, and we want to continue to be able to help them to do that.

Our experience in attempting to help or even obtain information on the extent of the problem in some sectors has been mixed. Some agencies, such as the electricity monopoly, have been open to technical exchanges, but for much of the Russian Government, transparency still comes hard. To illustrate, one key ministry refused to meet with the U.S. embassy officials to discuss their Y2K preparations because they didn't want to "spread rumors". We will continue to seek satisfactory answers on behalf of the many Americans who live in or do business with Russia.

Mr. Chairman, in conclusion, allow me to make a very few brief general points. First, in assessing Russia's overall vulnerability, it is important to bear in mind, as Chairman Bennett noted in his opening statement, that much of the country's infrastructure is less dependant on computer technology than is the case in the west. This fact tends to lessen the risk of large-scale systemic failures in favor of more localized problems that can be fixed more easily and more quickly. Unfortunately, this has also led to a certain complacency on the part of some in the government and financial community and tendency to understate the actual risk potential.

Second, the level of technical and engineering expertise in Russia is relatively high. Programmers and engineers are prepared to deal with the shocks and aftershocks as the millennium rolls over. These experts were schooled in the communist era of shortages

when the unavailability of replacement systems meant fixing and re-fixing and re-fixing again, and thus they have been compelled to become intimately familiar with their systems, and they can be creative and resourceful in dealing with novel or unanticipated problems.

But it is also important to remember that the Y2K problem is unprecedented, and it is of potentially large-scale magnitude. So even with the best will and capabilities, there are going to be too many problems to deal with immediately, and it is far from clear to us that Russia has sufficient resources to deal effectively with all the consequences.

How long might disruptions last? Russia may continue to experience Y2K-resulting problems in some sectors for months after the new year, as was noted earlier, and it could take some time for any temporary fixes to be replaced by permanent solutions. It is going to be prudent for us to view post-Y2K Russia in a similar way that we are viewing pre-Y2K Russia, as a country that may continue to rely on U.S. and other international help in overcoming computer related disruptions. We intend, of course, to maintain close contact with key Russian sectors before and after the new year to continually assess new developments.

Mr. Chairman, I want to thank you again for the opportunity to address the committee and for the leadership you and your colleagues have shown in maintaining a focus on what is really a critical issue that probably hasn't gotten the attention it needs, and we look forward to keeping in touch with you and the committee and your staff to help ameliorate the impact of Y2K on American national interests.

Thank you.

Vice Chairman DODD. Thank you very much.

[The prepared statement of Mr. Beyrle can be found in the appendix.]

Vice Chairman DODD. Mr. Warner.

STATEMENT OF HON. EDWARD WARNER, III, ASSISTANT SECRETARY, STRATEGY AND THREAT REDUCTION, DEPARTMENT OF DEFENSE

Mr. WARNER. Thank you, Senator. I am also very pleased to be here today to discuss the cooperation on Y2K issues between the Department of Defense and the Russian Ministry of Defense. I share with Mr. Beyrle the great respect for Senator Lugar. I am the latest of a number of individuals that have had the opportunity to administer the Nunn-Lugar Cooperate Threat Reduction program. It is a terrific program. It has played an important role. It has much wider scope, as the two of you discussed just a few minutes ago, and I would be happy to respond to any of your questions on that set of issues as well.

We have also appreciated the support of your committee, of both the members and the staff that from the very outset have helped provide us with the resources and certainly with the encouragement that we ought to be working with the Russians in this crucial area.

What I would like to do is I have provided a much more detailed statement, and I would really like to simply highlight some of the

areas in which we are engaged in cooperation with the Russians on Y2K. In your letter inviting me here, one of the questions you asked was what is the relative role of this cooperation in our overall pattern of cooperation with the Ministry of Defense, and let me say it has become one of the flagships of that cooperation during this year, which has been, thanks to our differences over Kosovo, a difficult year, but as I will note, we got underway our discussions with the Russians beginning as early as last fall.

We began to gather serious momentum with a meeting in February that scheduled a series of follow-up meetings later in the spring. Unfortunately, of course, given our strong national differences over the events in the Balkans, most of our cooperation with Russia was put on hold for several months. A single exception to that, by the way, was the Cooperative Threat Reduction program where, even in the midst of strong differences, the Russians found it most certainly worth their while to continue this very constructive and important cooperation.

Nevertheless, the re-engagement with Russia more broadly on defense matters didn't begin to occur until August, and again in the lead in that re-engagement with a couple of meetings on Y2K-related matters, as I will note in just a couple of minutes. By late August, we had a secured agreement from the Ministry of Defense to begin our broad agenda of cooperation once again and led to an important event on the 13th of September when Secretary Cohen visited Moscow and signed with Minister Sergeyev the joint statement to set up the Center for Strategic Stability for Y2K out at California Springs, and I will speak to that more in a moment.

We have a series of further engagements with Russian expert counterparts scheduled throughout the rest of this year, leading right up to the transition, and given the fact the transition itself will really not culminate only on the first of January, I am sure we will remain in touch with them in the months following that because the Russians, like us, have identified the opening quarter of calendar year 2000 as a critical one in this area.

Let me speak briefly about the five areas in which we are cooperating with the Russians through the Department of Defense. One of them is on direct communications or hot lines, first of which dates back to the one installed in the wake of the Cuban Missile Crisis in the sixties and others that have been added in more recent years. Another has been the discussion of the overall management of Y2K problems within our respective ministries, if you will. A third has been the question of nuclear weapon stockpile security, the one that Senator Lugar already referred to and I will speak a bit on this issue as well. A fourth had been the command and control of nuclear forces, and a fifth is the establishment of the Center for Y2K Strategic Stability that will be created in Colorado Springs.

On the question of hot lines, we have had a continuing relationship with the Russians, and we have increased the number of both data and voice links between the top leaders in our governments and between risk reduction centers that were instigated by the Congress in the mid–1980's. That work began almost a year ago. It has gone on with periodic meetings.

As we now reach the point here of the early fall, we have agreed on a series of measures. We are working with them to replace key software associated with the hot lines at our end and their end of these communications links. We are also, over the next couple of months, going to set up alternative circuits to sustain communication, including INMARSAT potential to be invoked if in fact the hot lines themselves were not to perform effectively and were needed in the time following the transition.

With regard to the overall management of Y2K matters, that is how we as a department have come to address the manifold challenges of Y2K, we began discussions with the Russians on this matter last February. It was disrupted by the Kosovo events. We resumed discussions in late August. It is clear that the Russians are interested not only in comparing notes on the manner in which one addresses, identifies, remediates, tests various systems with potential Y2K failures, but it is also clear that this is going to become an element of our sustained cooperation past Y2K.

The question of the management of information technology in this dynamic period, I think is going to become one of the elements of continuing discussion and cooperation between our two sides. On the nuclear weapon stockpile security matter, the discussions on that began as early as last fall, and they did so in the context of the Cooperation Threat Reduction contacts that we have between the Department of Defense on one hand and the Twelfth Main Directorate of the Ministry of Defense of Russia which is the one responsible for the safekeeping and storage of nuclear weapons. So we got off to an early start in talking with them.

As Senator Lugar noted, one of the things we encouraged them to do is to do a far-reaching assessment of their potential vulnerabilities to Y2K and to also identify appropriate means to deal with the potential charges. The Russians briefed us in August about the results of that assessment and their measures that they are currently undertaking and will have in place by the time of the Y2K rollover at the first of the year. They noted that they had come to believe that they needed to be attentive to the role of Y2K, particularly in how it might affect the microenvironments, if you will, and their nuclear weapons storage facilities.

They have agreed to set up—I mean they have set for themselves a goal of setting up some 50 monitoring stations at all of their main nuclear weapons storage area. They are also developing response capabilities on what they could do in case there is difficulty and they would need to have an emergency response to a problem that might arise. It is in this context that the Russians raised the issue that you, Senator Lugar, referred to a few minutes ago, the potential for direct financial aid from the United States in order to help them to procure variation types of equipment. Some are sort of office-related equipment for the 50 monitoring centers, but the majority are related to the question of emergency response, and they have talked to us about radio communications and various types of vehicles, fire trucks ambulances, weapons handling trucks, and the like.

As noted in my prepared statement, due to circumstances about the availability of funds at the moment, up to this time we have been able to locate $3 million, a million out of uncommitted Cooper-

ative Threat Reduction [CTR], monies from 1999 and about two million from the Y2K supplemental. If we can succeed in having recertification relevant to releasing the CTR funds and the signing of the Defense Authorization Bill, we will have other monies available to add to the three million.

Right now, we have prioritized within their request on how the use the three million.

If we are able to use additional monies, we will, in fact, dedicate those to the remainder of their list in order to provide them with these capabilities. We have already begun working with them on the contracting vehicles to be able to get this material in place as rapidly as possible, if at all possible by the time of the turnover. If not then, within weeks or days after that. We will continue to work on that program. We will look forward to working together within the administration and working with the Congress on the recertification issue here in the days ahead.

On the command and control of nuclear forces, when our large delegation on Y2K matters went to Moscow in February, we opened a dialog with them about the approaches we have been taking to ensure secure and reliable communications within nuclear forces. We resumed that dialog just last week when a senior officer from the strategic command went down the Colorado Springs and spoke with the visiting Russian delegation that had come to see the new center that will be established.

We are looking forward to sending individuals to Russia within the next month or so to really compare notes on the manner in which we have been doing operational evaluations of mission-critical systems and on the way we have developed operational contingency plans to address any possible failures in any systems that one identifies as at risk. We have had discussions with figures within the Russian Strategic Nuclear Forces, Major General Dvorkin and others, over the past many months.

It is clear Russia has been focused on this problem since late last fall. It remains to be seen to have more detailed discussions on precisely how they have handled it. It certainly has been a focus of their attention.

We do not believe—I share Senator Lugar's conclusion. We believe the chances are virtually nonexistent that Y2K failure would lead to the loss of control and the potential launch of a nuclear weapon. If anything, the system would probably lock up and make it less capable of launching weapons rather than more capable of doing so. But, nevertheless, we want to engage in a dialog with the Russians on this crucial matter.

Finally, let me say just a couple of words about the Center for Y2K Strategic Stability being established in Colorado Springs. You two gentlemen have already described the center in much the same words that I would. It is designed in order to have American and Russian military personnel sitting side by side from the latter part of December into the middle of January, monitoring data on the potential launch of long-range missiles or space vehicles from around the world. The data to be monitored will be provided by the American side.

Let me say for a moment and really answer a question you posed earlier, Senator Dodd, on whether this isn't a good idea over the

longer term. You may remember at the summit in Moscow a year ago, President Yeltsin and President Clinton, as a matter of fact, signed a joint statement to commit the two sides to develop and field a jointly manned warning center of a permanent nature between Russia and the United States that will be located in Moscow. We have had—had had productive initial negotiations with the Russians in February and again in March on the road toward the establishment of that center, and that center will, as a matter of fact, display data developed by the warning sensors of both sides.

In the case of the temporary facility for Y2K in Colorado Springs, we will be using U.S.-provided data only because we hadn't gotten far enough to be able to convince the Russians to provide their data to our center. On the joint warning center, we are looking forward to the resumption of negotiations on that matter within the next couple of weeks or few weeks. We have agreed with the Russians that this should take place. Both of us are preparing draft memoranda associated to the functioning of that center and a pre-launch notification regime that is going to be of an international character.

So I believe we will pioneer this concept of jointly monitoring launches and having then secure communications from that joint warning center, in this case from the temporary center in Colorado Springs to our own military authorities and then back into Moscow. I believe that the permanent joint warning center, it is likely we will complete the negotiations over the next 6 months or so, and we will work very hard to get it established sometime during the year 2000.

On a final note on the warning center in Colorado Springs, it will not only serve the purpose of monitoring the situation of global launches and having communications means to communicate with either side, and therefore keep any mishaps from becoming strategic miscalculations, it will also, because of the assured communications link, be a place where the defense establishments of both sides can rapidly be in contact with one another if any other Y2K-related issues may arise during the transition. So if the Russians prove, because of difficulties with their power sector or others, to have events that would be of military consequence, if they simply want to inform us of this or if they want to seek our assistance or expert advice on this, this will be a prime channel of communications to serve that purpose over the Y2K transition.

We have done a lot in this area. We have work to be done in these next few months to run up to and through the transition. It is thanks to the support of this committee, including the financial support made possible by the Y2K supplemental, that we have been allowed to do this. So we thank you for that, and we will continue in this effort.

Vice Chairman DODD. Thank you very much, Mr. Warner.

[The prepared statement of Mr. Warner can be found in the appendix.]

Vice Chairman DODD. Mr. Baker.

STATEMENT OF KENNETH BAKER, PRINCIPAL DEPUTY ASSISTANT SECRETARY, INTERNATIONAL AND NATIONAL SECURITY, THE DEPARTMENT OF ENERGY

Mr. BAKER. Thank you very much, Mr. Chairman and members of the committee for the opportunity to appear before you today.

Vice Chairman DODD. You have to bring the microphone right over to you.

Mr. BAKER. Thank you for the opportunity to appear before you this morning to discuss the Y2K problems at Soviet-designed nuclear reactors. In the interest of time and with your permission, Mr. Chairman, I would like to submit my full statement for the record and make abbreviated remarks.

I would also like to echo what has already been stated about Senator Lugar. He has been a leader to the Department of Energy of securing these nuclear materials, and also his Russian leadership has really paved the way for us already to secure over 100 metric tons of loose nuclear materials that is secured today.

This committee is to be commended for its work on Y2K issues in the United States and internationally. I look forward to working with the committee members to assist in Y2K problems that Soviet-designed nuclear power plants located in the new independent states and eastern European countries. These Y2K efforts are conducted as part of ongoing safety improvement activities at 68 reactors and 23 nuclear power plant sites.

I want to emphasize first that the department is providing assistance to these countries; however, we are not managing the Y2K remediation efforts. Department experts have held meetings with host country experts and visited several of the nuclear power plants to evaluate Y2K needs. Based on our experiences and observations of Y2K-related work being done at these nuclear plants, we conclude there is not a significantly increased risk of a nuclear accident at any of these Soviet-designed nuclear power plants due to the Y2K event.

Department experts anticipate that the primary safety systems, outlined on the board over here, at these plants will continue to function properly, and if needed, safely shutdown the plants during a potential Y2K event. There are, however, Y2K issues with other systems important to safety and normal plant operations, as Senator Lugar just discussed.

Also, I would like to stress that, irrespective of Y2K issues, there are many important safety problems that need to be resolved at Soviet-designed nuclear power plants. Our common goal is to help these countries ensure that Y2K events will not cause an accident or significant problem regarding plant safety.

The department's Y2K assistance addresses all the nuclear power plants and focuses on three main designs: the RBMK, the old Chernobyl-type reactor; the VVER–440; and the last, the VVER–1000. These reactors are located in nine countries: Russia, Ukraine, Lithuania, Armenia, Kazakhstan, the Czech Republic, Bulgaria, Slovakia, and Hungary. Russia, Ukraine and the other seven host countries have established Y2K programs.

We have categorized these programs into four partially overlapping phases: one inventory and preliminary assessments of what they have that could be Y2K incompatible, a detailed assessment;

phase two, analyzing these and find out what really needs to be fixed. The third phase is remediation, replacing hardware, software; and the final phase and probably most important phase is contingency plans, how do we plan and make contingencies against the worse case.

Of the 68 nuclear reactor units in nine countries of the former Soviet Union, 50 have been completed with Phase II assessments and testing. The remaining nuclear units are in the process of completing the detailed assessments and testing activities. Of the 68 reactor units, 45 have begun their contingency plans. Based on current information, there are no known Y2K problems with a primary reactor safety systems at these plants. These systems detect problems and automatically shut down the plant. We expect that the primary safety systems will function properly and shut down the plants safely without regard to Y2K issues.

The countries are at various stages readiness. Russia has established a well-organized and aggressive but underfunded Y2K program. Each plant reports that it has completed its preliminary and detailed assessments, although we are not certain of the death and comprehensiveness of those assessments. The nuclear power plants in Russia plan to complete remediation of their important safety systems next month. Ukraine has developed an assessment program but until recently has only completed limited assessments.

The department is partnering with the science and technology center in Ukraine to work with a Ukrainian utility and nuclear power plants to implement Y2K assessment methodology similar to the one described in the IAEA guidance document. And here is a copy, sir, of the IAEA guidance document that has been passed out to all countries. It lays out all those four phases which I just talked about.

Y2K concerns do exist in systems that are important to safety at Russian and Ukrainian power plants, however. One concern is the plant processing computer common to both the RBMK and VVER reactors. This computer monitors the reactor and gives information to the operator. The operator uses this information to make needed adjustments to the plant, such as moving control rods and closing and opening valves to control flow rates of cooling water to the reactor. Failure of the plant process computer is not an immediate safety concern, but regulations require that the plant be shut down, like Senator Lugar said and you said Senator Dodd, in 90 to 120 minutes, within a few hours, if this computer is not restored to normal.

RBMK plant process computers are known to suffer from both hardware and software Y2K vulnerabilities. The VVER problems are, however, only to the software side of Y2K. There is concern that if not fixed, these and other problems could result in simultaneous shutdown of several nuclear plants, causing disruption of power supplies in the middle of winter. The shutting down of the reactor could have serious impact on the populous.

Russians report that they have assessed the plant process computer software vulnerabilities and can use a manual process. Work is in progress in Ukraine to assess the same problems, using special software tools provided by the department. The department is

working with both countries to remediate Y2K problems with the plant process computers by the first of November.

The department has discussed with Russian and Ukrainian Government officials the need for sufficient supplies of diesel fuel to power the generators needed to be operated safely in the event of offsite power loss for Y2K. U.S. experts are meeting with the nuclear power staff to assess the adequacy of diesel fuel supplies and to help prepare against potential offsite power loss. Host countries are working with the department to develop contingency plans to address this concern. These plans are intended to help plan operators under potential Y2K problems and establish the procedures to address them. The plans would help prevent operators from inadvertently making a situation worse through the inappropriate operator actions which happened in Chernobyl.

Based on the meetings at the International Atomic Agency [IAEA], discussions with the host countries, the countries of Bulgaria, the Czech Republic, Hungary, Lithuania, appear to be adequately addressing Y2K issues. Kazakhstan has permanently shut down their BM–350 reactor, limiting the need for Y2K assistance; hence, the department is focusing on the countries of Russia, Ukraine, and Armenia.

In Russia, the department's efforts complement those of the International Science and Technology Center. The center is pursuing a program at Russian nuclear power plants to help verify Y2K assessments that Russian nuclear plants will have completed the guidelines. The center plans to complete those assessments that are either deficient or completed in the month of October.

The department's Y2K effort in Ukraine is conducted in partnership with the Science and Technology Center, the Ukraine Institutes, and the nuclear power plants. Based on these assessments, the department is currently responding to requests for remediation assistance from Chernobyl.

Nuclear power plants in Ukraine: We anticipate that the remaining nuclear power plants in Ukraine will have similar requests for remediation assistance, and as their detailed assessment work progresses, we will provide assistance and correct the most serious deficiencies needed for remediation. Now that remediation actions are under way, the department has begun to assist host countries in completing their contingency plans. During this phase of the department's assistance, we expect the highest priority vulnerabilities of the Soviet-designed reactors to the Y2K event.

Our contingency information is that the loss of offsite power is at the top of the list. The department's contingency planning support will address this issue. We are relying on host countries to assess the Y2K issues properly and remediate these problems and develop contingency plans within the last few months. We have provided information and assistance at each step along the path to Y2K readiness.

The initial complacency that was expressed by the host country representatives has given way to significant efforts to help resolve this problem. We have got their attention. In the light of a relative late start of the Y2K activities, we cannot be completely certain that they will be successful, but we do anticipate the failure of the primary—we do not anticipate the failure of the primary systems,

therefore the department believes that there is not a significant risk, increased risk, of a nuclear accident at a Soviet-designed nuclear power plant due to a Y2K event.

We will, however, continue to work with the committee and others to help resolve Y2K issues that have been identified at Soviet-designed nuclear power plants. We will continue to provide other types of assistance to improve the safety of these plants since deficiencies remain in the design, as Senator Lugar said, equipment training, and operational procedures.

This concludes my statement, sir. I would be happy to answer any questions.

Vice Chairman DODD. Well, thank you very, very much.

[The prepared statement of Mr. Baker can be found in the appendix.]

Vice Chairman DODD. I thank all three of you for your contribution to this hearing this morning. The chairman of the committee, Senator Bennett, is up at the Banking Committee on a hearing there of some importance. I am a member of that committee as well, and I am going to ask one or two questions and then quickly turn to my colleague from Indiana. I will slip out and go up to the Banking Committee. Senator Bennett, I think will come down, and we will try to keep this moving here so as not to disrupt the flow and hopefully not be repetitive in our questions.

One question comes to mind immediately, Mr. Baker. I saw where the secretary is in Russia today, in fact, and is there until Friday on energy-related matters and is touring nuclear non-proliferation programs set up to deal with vast stockpiles of nuclear material. Is the Y2K issue on that agenda of that trip? I hope it is.

Mr. BAKER. The Y2K issue is on that agenda, sir. He is talking to Prime Minister Makolov about the Y2K issue. It is very high on his list. Of course, he is there looking at facilities, the work we are doing with the Russian Navy and the other materials, protection, control, and accounting, but the Y2K issue is very high with the secretary, and we are really working very hard with the Russians. We have over 45 programs that we have worked with the Russians in the Y2K area, and it is very high on the secretary's list.

Vice Chairman DODD. Well, great. Well, you, I am sure, will be in touch with the office this week, and you might communicate through the appropriate channels that this committee is deeply interested in what he learns during these next few days, and we would love to be briefed, if we could through staff or otherwise, as to what he learns as a result of this. And there may be some questions that come up today that would be appropriately transmitted to him as a level of concern being expressed by members of this committee.

Mr. BAKER. Yes, sir. I will pass that on.

Vice Chairman DODD. Let me jump, if I can, very quickly, and then I will ask this one question, and then I will let my colleague from Indiana pick up, and I will come back. This report that was done under contract with the Department of Energy, the Pacific Northwest National Laboratory report in May, I presume you are familiar with this.

Mr. BAKER. I am familiar with a lot of contracts with Pacific Northwest Labs, sir.

Vice Chairman DODD. This is one they did, the worldwide assessment, the vulnerability of nuclear power plants and electric power grids to the Y2K bug, was the report that was done. I can just tell, without you turning around, there are some heads behind you saying, yes, we are familiar with this. So I know that feeling. My staff does that as well.

Mr. BAKER. Yes, sir. He is my engineer.

Vice Chairman DODD. Well, and again I appreciate the comments here, the level of optimism you have expressed both at the outset and the conclusion of your remarks about any kind of serious potential failure here due to the Y2K issue.

I would like to clarify, though, and you touched on it here, the RBMK reactors or the Chernobyl-type reactors, which I have mentioned and you have mentioned, and again human error played such a critical role there in that tragedy, there are 11 of these at three different locations. According to experts in this report, anyway, they can only withstand, as you point out and I mentioned in my opening remarks, a power loss of 90 to 120 minutes. What precautions are the Russians taking so that this doesn't happen? Because we have heard there may be these disruptions that will occur in the grids, and if you lose power for an hour and a half or 2 hours, then you do have a serious problem.

Mr. BAKER. What we are doing, sir, as you say in this type reactor, we are fixing two things right now. We are fixing the process computer. We are building new software. We have got scanning tools to make sure that software, that process computer in that Chernobyl-type reactor is fixed. We also are putting in a new hardware system, computer system, in the data system in the Chernobyl-type computer, and what that does is monitors the core at all times to make sure that if there is anything wrong, these things will be compatible, and the operator will have—providing everything goes the way we are doing it right now, will have readable gauges that are accurate.

Now, what are we doing in case offsite power is lost? Well, first of all, the plant operators have assured us that the populous will lose power before the reactors will lose power. That is one. We have got that assurance from the Russian Government. No. 2, we are putting in extra diesel fuel for these diesels to operate so if something is shut down, the diesels will startup.

What we are looking at right now in the contingency plan is to start these diesels 2 days before the year 2000 to make sure they are running when the Y2K hour comes. So we are doing a lot of this contingency. Operators are being trained. We are looking at operators' procedures. So the things that happened in Chernobyl, like operator error, they failed to read gauges, I think all of this has been trained out, and the contingencies we are building right now will safeguard against this as much as one can.

Vice Chairman DODD. OK. And very quickly, Mr. Beyrle, if I could, your testimony indicates that depending upon the severity of Y2K problems in Russia, the U.S. will need to, and I quote, come to a decision on the most effective response. I wonder what thresh-

olds or policies currently exist which would expedite the kind of decisionmaking.

Mr. BEYRLE. Well, Senator, thank you. As we look at the problems that, you know, are starting to come into sharper focus, we are trying to get as much information we can in the first instance from the Russian Government, Russian agencies, on what they see the scope of the problem as being.

Vice Chairman DODD. Can you bring that microphone a little closer to you?

Mr. BEYRLE. And how they are set up to deal with it. At the same time, we are consulting internally, inside the U.S. Government obviously, as part of the committees and the commissions that have been set up to deal with this and also multilaterally with our allies, with the EBRD, with the international financial institutions to try to come up with strategies and policies to deal with this.

For instance, I think beginning next week or the next 2 weeks in Prague and culminating in mid-November in Vienna, there will be a series of meetings in which we are bringing together the operators of electricity grids in central and eastern Europe and the energy providers to try to get them together to share expertise and solutions, put them together with our experts to give them a sense of how we think that ought to deal with the problems. We use those forums as a way to get a better sense of what the problems might be, but I have to say at this point we are still gathering as much information as we can, and we are going the need to continue in that effort through the millennium rollover and after.

We need to prioritize. We need to come up with strategies to deal with the disruptions that are going to hit our national security interests first and foremost. Those are the priority things that we have to deal with, the nuclear questions that my colleagues have talked about.

The second order of priorities, the economic and humanitarian considerations, we will also have to deal. There are finite resources, obviously, that we have to bring the bear on that, but we probably are going to need to work out a fairly well-thought-out policy framework, prioritized policy framework for responding to these problems.

Vice Chairman DODD. We have got about 66 working days, I count. I mean 94 days, but working days, and then we are going to be out of session here, some would hope earlier than later, but fairly soon, I presume sometime around the first of November or shortly thereafter. So we will be, in terms of the Congress's ability to initiate, to enact legislation and things that may be needed—now, obviously, there may be contingency funds and other ways of getting around it, but you can appreciate my sense of some concern here.

I will let you comment as I go out the door on this, but my concern is that coming to a decision process with so few working days left on how you prioritize, and I think you have stated it well. I agree with your initial prioritization that you have made here as to what is important. I just get a little uneasy about our ability to actually respond, to the extent that we want to be able to respond,

to provide the necessary assistance. It is just getting so short in terms of time.

Mr. BEYRLE. No. I agree with you entirely, Senator, and a lot of it depends on the Russian Government and Russian agencies, how forthcoming they are going to be in being up front with us on the problems that they haven't addressed yet, and the problems that they foresee coming down the road may be, as we have talked about, 30 to 40 days after January 1, 2000.

This is an iterative process. We are not going to have anything close to all the answers even on January 1st. We will need to stay in touch with the committee, obviously, because there may be resource implications for us. Clearly, we are going to want to try to help the Russians deal with this problem through continually providing expertise, hardware, and training, but there aren't unlimited resources for that.

Vice Chairman DODD. I apologize. Thank you.

Chairman BENNETT. I told the Banking Committee Senator Dodd and I are doing tag team. I stayed there until I questioned, and then I am down here, and he is back up there. I apologize not having been here. I have no brilliant questions.

Senator LUGAR. Senator LUGAR. Well, Mr. Chairman, I would like to ask Mr. Warner, we have had a great deal of discussion about the value of Russian and American military officers sitting side by side in Colorado Springs or in the more ambitious program that you have been negotiating, but what assurance can you give the American people that while they are sitting there side by side, that strategic interests of the United States, our early warning capabilities and what have you, are not compromised?

Mr. WARNER. We are ensuring both in the temporary center to be established in Colorado Springs and as we negotiate the modalities for the permanent facility, if we do reach closure on that, that will be established in Moscow, that in both cases we will provide in a sense what we call filtered data from our sensors, both space-based and ground-based radars and infrared detectors.

Senator LUGAR. Filtered data?

Mr. WARNER. Filtered data means that it will be adequate to most certainly say there has been a launch, approximately where it is been, what is the direction in which the missile in question seems to be proceeding, and even a broad projection of the potential impact area. We can do that in ways, and we have worked closely with the space command and other military experts on this matter to ensure that the filtering means that it is adequate to the task, but it does not by any means reveal internal critical characteristics of our sensors.

Senator LUGAR. Mr. Beyrle, in your testimony, you have pointed, I think correctly, that power generation and telecommunications are the areas of greatest concern, but can you give some idea is the State Department continuously planning a risk assessment of what these failures may mean? I cited the American Chamber of Commerce estimates that as much as 40 percent of transportation could be affected for a period of time, likewise, the chunks in telecommunications, banking system, the securities markets.

In the event that these situations come to pass in that degree with that large of a portion of the Russian economy or the Russian

people being poorly served, this is likely to have a lot of implications as to life in the country during those weeks and months, that is the ability of local governments to maintain control or even more difficult ramifications as life becomes so grim people take desperate measures of all sorts. What kind of thinking is the State Department doing, or what sort of discipline are you applying now to try to think through what happens in Russia if these things come to pass, leaving aside whether the Y2K thing is being remediated in as rapid a way as possible?

Mr. BEYRLE. Well, Senator, we are obviously concerned about some of the worse-case scenarios that you have alluded to there. I think in the first instance, we have tried to impress upon the Russian Government the importance of communicating with its own people what the realities of Y2K may be and what the worse-case potentials are.

Senator LUGAR. To what extent are they doing that? What evidence do you see of that?

Mr. BEYRLE. Frankly, as I mentioned earlier, the fact that a recent poll indicates that 50 percent of the Russian people aren't even aware of the Y2K problem is indicative of the fact that they have a lot of work to do. We understand from our contacts with entity in the Russian Government which is charged with civilian disasters, civilian emergencies and natural disasters, that some areas of the country are beginning to stockpile fuel, for example. We heard about stockpiling diesel fuel in connection with nuclear plants.

But it is, frankly, to our judgment at this point, not enough. Much more has got to be done on this. I think with respect to your question about disruptions in telecommunication and the effects that this could have on business transactions, on essential services, health, security, communications, there is also, obviously, a tremendous potential for disruption. I don't think that we won't see this necessarily leading to unrest in Russian society.

Russians are somewhat accustomed to dealing with failure, to making due through hardship. That is a somewhat glib response that maybe ignores the reality that we may be looking at a situation, where for two or 3 weeks people don't have telephones, people don't have electricity in their homes.

Senator LUGAR. There are, as we have cited, maybe as much as 11,000 American citizens who are in Russia presently. Perhaps this understates the number. What is to happen to them in this period of time? Would your advice be to leave the country, or how do they cope?

Mr. BEYRLE. We have recently put on a consulate information sheet to the general public and made it available to citizens living in Russia, and also on the State Department web site, which advises citizens to take precautions and to prepare to cope with the disruptions that may come to pass. We have tried to be very straightforward with the U.S. public living in Russia that disruptions are likely, but as someone has pointed out, the Y2K problem is somewhat the mirror image of a natural disaster, as with an earthquake. You know what is going to happen. You may not know when, but you know what is going to happen.

Y2K is the opposite. We know when it is going to happen, but the consequences aren't exactly clear. So we are trying to warn American citizens simply that there is a potential for disruptions and that they need to take precautions accordingly.

We do have every intention of keeping our embassies open and staffed to provide the information services that Americans are going to need during this time. There is no plan at present for any draw-down of staff in Russia or any of our consulates. We are still assessing the situation. If there were changes on the ground that forced us to reconsider that, we would still maintain our embassies and consulates open, and we would still maintain a level of essential services and essential staffing to deal with American problems.

Senator LUGAR. Well, that is very important. Obviously, you try to communicate with each one of these citizens, and the Russian Government is apparently beginning to try to communicate with its citizens, but as you pointed out, those outside of Moscow, St. Petersburg, or urban areas, may be the most vulnerable, and these may be the last to get the word in terms of the Russian communication system.

Likewise, what thought has the State Department given as to in the event that these remote areas have extraordinary suffering or even seemingly are cutoff by communications from other parts? Are Governors of those areas capable of managing on their own? In other words, if the central government fails in this sense or really is ineffective, what is the status of the rest of Russia, the components as people try to deal with this?

Mr. BEYRLE. Well, obviously inherent in your question is the realization and the reality that the decentralization that has taken place in Russia since the fall of communism has helped the situation in that the regions are a bit more self-reliant now and have more autonomy and probably more independent decisionmaking capability. Whether they will have the wherewithal to cope with these problems is another question.

Frankly, these are questions that we are only now beginning to wrestle with. These are the kind of worse-case scenarios that we, in the first instance, need to engage with the Russian Government on. We need to ensure that they have thought through the worse-case scenarios themselves and are beginning to put plans in place to deal with them. It is not a problem that we can solve for them. We can provide help and assistance, but we need to make sure that they are focused on the problem.

Senator LUGAR. Hopefully, if the Russian Government is monitoring this hearing, this will be helpful to indicate that we are concerned, and we believe they ought to be, because it is a very serious matter, and they should be.

Mr. BEYRLE. I think you are right. This is one of many ways we have of getting the message to the Russian people and the Russian Government.

Senator LUGAR. Mr. Baker, just one follow-up question of Senator Dodd's query about nuclear plant failure. What are the problems or the increased risks of radiation release in all of this? At some stage, that is not the only fear people have of these instruments, but it is a major one, and after a certain amount of shutdown, the

danger of that obviously increases substantially. What is your own analysis?

Mr. BAKER. Well, Senator, you know, the RBMK-type reactor does not have a containment device. The VVERs do have containment devices, so radiation, you know, cannot escape if something went wrong, but we hope—and we have been working, like I say, day and night with all these committees involved. There is over 45 committees involved with the IEA and involved with the Department of Energy on making sure that reactors operators have the current procedures, that they have been trained, that the software and the hardware will be fixed in these two units that I just talked about so if something goes wrong, they can shut it down immediately.

We have the primary system that is an analog system that will shut down immediately. So we think the radiation would be controlled, that if something goes wrong with the system, all it takes the pin rods going right down into the reactor, and it stops instantaneously.

The big concern, of course, like the worse case-type concern, is where you lose offsite power, and power is not provided to the reactor and the diesels do not startup or the batteries do not work and then the cooling system does not get to the reactor and the reactor melts down, but that is the worse-type scenario which we don't think there is hardly probability of that right now, but what went wrong with Chernobyl was about everything. They didn't follow their gauges. The reactor, they tried to bypass some gauges that gave different readings. So it was a training problem. It was a procedure problem, and it was a reactor problem, and hopefully those type things have been overcome.

As I mentioned to you before, the reason—reactors in Russia do have—are more dangerous than in the United States. We say in our opinion they are 100 times more dangerous, but, again, we are doing the same things at the Department of Energy as, you know, in our nuclear safety program, and as you mentioned, design equipment, training, operational procedures. So we are saying this Y2K event on top of it does not increase the risk, but we need to keep working like we have been working on nuclear safety because we need to fix the Y2K problem, and I think we have.

We are not saying, sir, we will be finished in January, because you have got other safety systems that don't have such a high priority as these that will not be fixed complete by 1 January; however, the primary and the backup systems, so that we won't have some type of catastrophic failure, we think have been fixed.

Senator LUGAR. Well, I thank you, Mr. Baker. Your testimony and that of the other witnesses underlines the fact that rapidly in this room we have gotten over whether the United States and Russia should be cooperating. The question is will the intensity of all that cooperation, every safeguard we are attempting to institute at the Department of Energy or Department of Defense get there in time, but I congratulate the chairman again for simply pointing out that this is the issue, the quality of the engagement, not whether there should be engagement, because this is a crucial time for both of our countries.

Mr. BAKER. I agree with you, sir. The worst enemy is time right now.

Chairman BENNETT. Thank you very much, Senator Lugar.

I may have some additional questions, but I will submit them to you in writing because I was not here to hear your testimony, and thank you very much for being here today.

We will now proceed to the final panel. We have heard from Senator Lugar as our first panelist, the global overview. Then we have heard the governmental view from State, Defense, and Energy. Now we are going the hear from some private citizens who have expertise in the area.

We welcome to the committee Mr. William McHenry who is an associate professor at Georgetown. He has been studying Russian information systems since 1978 and is joined by Mr. Richard Conn who chairs the legal committee of the U.S. Russia Business Council, and is a lawyer as a partner at the firm of Latham & Watkins. Gentlemen, we appreciate your patience, and we appreciate your willingness to be with us and share your expertise.

Mr. McHenry, we will start with you.

STATEMENT OF WILLIAM MCHENRY, ASSOCIATE PROFESSOR, MCDONOUGH SCHOOL OF BUSINESS, GEORGETOWN UNIVERSITY

Mr. MCHENRY. Chairman Bennett, Vice Chairman Dodd, and members of the committee, thank you for inviting me to testify. In the interest of time, I will abbreviate my remarks and ask that my whole statement be included in the record.

Chairman BENNETT. That will be done.

Mr. MCHENRY. Thank you.

This problem in Russia is taking place against the backdrop of extraordinary economic problems, as we have been discussing, and considerable political uncertainty. Indeed, the outlook of Politician Gregory Yavlinski was heard remarked that Russia's real Y2K problem is actually Boris Yeltsin, but we have to think really what impact and potential failures have against such events as the gross domestic product declining 4 percent since 1991 or, for example, the unified electrical system saying it only has 60 percent of the fuel oil it needs for the fall and winter season of this year.

Let me begin with my overall assessment. I agree with the assessments that have been made so far today that there will be a certain number of outages in various systems, but I also believe they will be local and contained and will not have an immediate dramatic long-term effect on the economy, especially in comparison with the other sources of problems that we have. I liken the impact to the number of blows that are coming during the boxing match. Many other blows are coming from other sources, and it is difficult to say just which blow might knock out the fighter.

I think over the longer term, the key question is whether or not there is any silver lining effect that comes from doing the remediation work. I believe that the Y2K problem may lead to greater economic efficiency, so I think on the one hand we may see some short-term visible effects. In the longer term, the effects that could be more serious would be more economic inefficiency. So let me talk about why I believe this is true.

First of all, as I have outlined in my statement, there have been delays in getting the work started. I have gone into considerable detail about that. By July, the estimate was that there are 150,000 systems in the government as a whole, and about 30,000 of these needed to be remediated, of which about 10,000 or 30 to 35 percent had already been remediated at that point in time. So if you look at the systems that they are going to be repairing by January 1st, it immediately leaps to mind the fact that there are a number of systems that they are simply skipping remediation work now that they don't consider to be critical. and that is one of the main sources of the fact that I believe there will be more economic inefficiency that comes about in the months after the year 2000 comes when they will have to deal with addressing those systems as well.

Second, in addressing the effectiveness of government policies, I want to mention that there has been enormous amount of work that is being done now and especially since the beginning of 1999. You can see a mobilization that has occurred, and the mobilization is in the area of sort of an administrative approach to the question. It sort of resembles the old campaigns that they had in Soviet times, and one of the things that they did was that organized a network of centers of competency which were designed to provide a visible place where organizations could go to get help for the Y2K problems.

They have been certifying all sorts of different software packages. They have been certifying hardware, especially personal computers, but the one thing the government couldn't do was to provide a lot of funding to these organizations, and since the centers required payment, this reduced the number of clients dramatically who were willing to come to them.

They also represent a mix. Some of leading systems integrators, but others are remnants of the Soviet system and do not have a particularly good reputation. By June 1999, they were present in only about 51 percent of the administrative regions of Russia. So I also—you know, this is additional evidence that there are some regions that have not received the necessary attention, and there has also been some movement to provide incentives, legal incentives. This has been a second crippling factor that has stopped the Russians from really taking a timely approach to this.

But in July, Boris Yeltsin rejected a law that had been passed by the Duma and the Federation Council about the Y2K situation. So that leaves just an order that he signed in June and a lot of orders that have been signed by the State Committee on Telecommunications which is now the lead body that is working on this.

The third is the question of financing. I think it is interesting that the government has consistently given very different estimates about the costs. First, it was 500 million. Then they said it would be two to three billion dollars. Then in May, they said it was $657 million. In June, they said it was $471 million. In July, they said it was $538 million. Now, what this says to me is that a lot of work is going on. It says that ministries have been refining their estimates. They have been getting more precise information. They have been carrying out the inventories of the systems. But also, of

alarm is the fact that as of July, only 15 percent of the funds or about $80 million had been spent.

Just a couple of days ago, the Duma approved a new bill to appropriate $800 million—I am sorry—up to $80 million for Y2K remediation, and that is awaiting the approval of the Federation Council and Yeltsin's signature. So this is the first time that the legislature has actually appropriated money. All throughout 1999, the monies have had to come from the budgets of the ministries themselves.

Also, a recent development is the State Committee on Telecommunications has finally been given the green light to seek a $50 credit to buy hardware and software in the west for possible delivery in October or November. This is something that has been discussed for many months, but it is different to believe that any systems based on this equipment would be able to be ready by January 1, 2000.

And, as we have discussed, very limited information is available about private firms, how much they have taken up they problem. However, a representative from Novell recently told me that they have seen a very large rise in business from government institutions and industrial enterprises in the second and third quarter of 1999, and that official at least believes that 90 to 95 percent of their customers will actually be ready.

Now, in terms of the energy area, the unified energy system has taken a very serious approach, in my opinion. As of July 1999, they were saying that 35 percent of their critical systems had been modernized or put back into service, but they had only spent about 20 percent of the $30 million they felt was necessary. The oil and gas companies seemed to be in better shape with much lower percentages of unremediated systems.

The central bank has reported that 80 percent of banking organizations have now remediated and are testing their systems, and evidence of that is that they have been able to carry a large-scale integrated test involving four different regions of the country. I believe that there is enough work going on there, and it has been going on for long enough and that the package software has been remediated that we don't expect a major meltdown there.

In the telecommunications sector, I agree that there are major potential problems there; however, again, the FAPSI which is the sort of former KGB arm for telecommunications, stepped in in July and began testing local telecommunications systems, and in this administrative approach, the pressure is being put on, and typically, you know, the history of the Soviet system is when attention is focused on certain problems in a very specific and very focused way, that they tend to fix those problems. They can't fix all of the problems that arise in the economy, but they can do the ones that are the most highest priority.

So I am a little bit more optimistic than what has been said so far in the hearing today. I believe that in measure of the risks that are involved, that they will be able to remediate the major systems that need to. So let me finish by talking about the longer term impact on the economy.

I believe that there are less noticeable effects which will increase inefficiency due to local infrastructure problems, due to manual

processing that may be necessitated by internal systems that don't work or insert bad data or because new systems haven't been purchased and that there will be the continued need for those other systems that won't be ready that they have had to put to the side for the time being.

So I believe that we should focus in our policy area in first of all making sure that we do the kinds of things that we have talked about, in forestalling catastrophic failures for areas like nuclear power plants, but then we have to choose what kind of silver lining we might want to provide for them. and I am of the opinion that a lot of economic activity in Russia takes place through barter. It is helping to keep alive a lot of enterprises which are not providing positive economic benefit for the economy. So if we were to provide resources to replace the computers that are in those enterprises, we might actually simply be prolonging the agony of that sector of the Russian economy.

On the other hand, giving help to small businesses that have no means to carry out remediation could be a way to provide the same kind of silver lining that a lot of western firms have been getting from this, and these include the most aggressive users of the internet, which may number about 1.5 million right now, and businesses that are more vulnerable to economic shocks because they are dealing in case rather than in bartered goods.

So, in conclusion, let me say that any time we speak about the longer term impact of policies in Russia, we have to think about how to encourage the formation of the necessary conditions for true economic reform. Many believe that an important part of the answer is building the civil society based on the rule of law that protects business activities in a stable climate. Investment in basic institution-building, such as education, may be a better long-term use of funds than supporting Y2K remediation expect in the most critical areas. Without stronger fundamental institutions, the Russian economy may still be lurching along from one crisis to the next long after the Y2K problem has faded from memory.

Thank you.

Chairman BENNETT. Thank you very much.

[The prepared statement of Mr. McHenry can be found in the appendix.]

Chairman BENNETT. Mr. Conn.

STATEMENT OF RICHARD A. CONN, JR., U.S.-RUSSIA BUSINESS COUNCIL, PARTNER, LATHAM & WATKINS

Mr. CONN. Good morning, Mr. Chairman and Senator Lugar. I am appearing before you today in my capacity as the chairman of the Legal Committee of the U.S.-Russia Business Council, an organization made up of approximately 250 U.S. companies active in Russia. It is a great pleasure and honor to provide a perspective on the potential effects of Y2K upon business in Russia in the short term and long term based on my years living in Russia in the early 1990's through the mid–1990's and my work on behalf of clients since then.

It is important, in my view, to begin by putting in context Y2K problems as they affect Russia. Since we have been discussing different analogies, I would look at Y2K as simply a part of a tidal

wave that has hit Russia over the past several years and would note that whether that tidal wave is 31 feet or 30 feet may not make that much of a difference to the typical Russian.

It is difficult to keep track of the number of governments that Russia has had come and go over the past 2 years. During that same timeframe, Russia suffered a knock-out economic blow which you, Senator Bennett, alluded to. With the simultaneous difficulty of its government debt and massive devaluation of its currency, Russia's banking system, which never had been particularly robust, was left in a shambles, causing even greater reliance upon barter, an inefficient economic system.

The world came quickly to see what happened to those involved in Russia for some time, namely that the Russian Government was virtually bankrupt, living off of borrowed funds, and Russia had an insufficient economic base from which to service its debt. Russia simply had not sorted out precisely how it was going to make a living, and to date it has still not succeeded in producing significant goods and services either for its own consumers or for foreign consumers to buy.

More recently, Russian governmental structures have suffered a crisis of confidence as the world has come to see with ever greater skepticism that information provided by Russian governmental entities is questionable. On top of this, regional disputes in Russia have boiled over into the heart of Russia's capital as terrorist bombs have turned Moscow into an anxious city, cracking down on people whose physical appearance categorizes them in the minds of law enforcement as sympathetic to the views of southern republics.

It isn't hard to understand why Y2K issues have not registered in Russia with the residents that they have in more developed western countries. Indeed, as a matter of priority, that the U.S.-Russia business council itself attempted to establish with Russia, Y2K has not in all candor been near the top of the list. This is not due to our view that Russia will avoid hardship as a result of Y2K. It will not. But rather, because of the political reality is such that Russia simply cannot focus significant attention on this issue, due in part of the press of other matters and also to the lack of financial wherewithal to address the problem, even if it wished to do so.

For these reasons it is perhaps surprising that Russia has done as much as it has to address Y2K matters. As noted in my written statement, there are certain sectors of the Russian economy in which Russia has made some progress, particularly with respect to large companies where financial resources and understanding of Y2K issues are greater.

I concur with the assessment of my colleagues at the American Chamber of Commerce in Moscow which were quoted at length by Senator Lugar. These provide a sense of the gravity of the situation. In addition, I view the State Department's perspective as a fair prognosis of Y2K's effect in Russia. The State Department noted that the country appears to be somewhat prepared to deal with Y2K problems but anticipated disruptions in key sectors of electrical power, heat, telecommunications, transportation, financial, and emergency services.

In response to these reports, Russian officials characteristically played down the potential for disruptions. They continue to main-

tain that computers which support Russia's vast infrastructure continue to be checked and worked upon to prevent the bug from disabling key sectors. The credibility of these reports, in my judgment, is weakened by inconsistencies and lack of verification.

Let me turn, then, to likely steps that we can see in the final days of this year from Russia. As outlined in my written statement, there are a variety of steps that Russia can take to continue the preparations it has already undertaken to deal with Y2K matters. These include, for example, setting up a committee to coordinate emergency measures as they arise now and in the beginning of the year 2000.

I believe it unlikely, however, that Russia will significantly gear up its efforts at this time. The reasons for this are essentially the same reasons that explain Russia's failure to act decisively to date. These include five factors: first, the lack of financial resources which were alluded to by my colleague. Russia has already reduced its estimates with respect to the cost of Y2K compliance from somewhere in the area of one to three billion, down—at least the latest I have heard—to below $200 million at this stage and without explanation as to why those estimates have been reduced; No. 2, ongoing lack of governmental leadership and coordination; No. 3, lack of political rewards for dealing with Y2K issues; four, other issues that are perceived as more pressing from Russia's perspective; and five, a cultural bias against reacting until a problem is clearly manifested.

Accordingly, while we can all hope to see greater progress during the next couple of months, we should not expect any type of additional effort over that time. Again, I would except from that the matters that Senator Lugar was alluding to previously dealing with security and energy-related matters having to do with nuclear safety issues.

As to short-term effects upon the Russian economy and potentially upon U.S. business, Russia's severe and economic political difficulties unquestionably pose the greatest threat to its citizens during the cold and dark winter months ahead. Last year, for example, there were many regions of Russia that were simply unable to obtain the basic necessities of food and heat during the winter months. The last thing that Russia needs is a Y2K bug that can only make matters worse. Unfortunately, that is precisely what Russia is going to get.

Accordingly, I believe that in the short term the combination of existing difficulties and the added Y2K-related failures will make more severe and more widespread the electrical power, heat, telecommunications, transportation, financial, and emergency service failures that had been visited upon Russia in the past. It is, however, noteworthy that since all of these sectors traditionally suffer period failures within Russia, it is probably not likely that Russians themselves will perceive the failures as magnitudes more severe than during last winter or that they will ascribe failures to Y2K.

Moreover, the ability of Russia to deal with inefficiencies and political and economic failures through working around problems, combined with their pride and being able to withstand hardship, will work to minimize the manifestations of Y2K within Russia. In

addition, the effect upon Russia will, in some small way, be cushioned by the fact that some Russian technology was purchased from the west in recent years and is Y2K compliant.

More significantly and on the other hand, a part of Russia is simply not linked in with the high-tech world, and therefore is unlikely directly to feel the effects of Y2K. The country, of course, will indirectly feel those effects through the lack of basic supplies as an already highly inefficient economy grinds even more slowly.

Turning then to long-term effects, after adjusting during the first half of the year 2000 to the effects of the Y2K bug, it would not be surprising to see the issue largely disappear from the political and economic extreme in Russia as it is overtaken by more high profile issues. Russia may well find itself paying the price for creating an unattractive investment environment that has driven away domestic and international investors, as well as domestic and international talent from Russia. This may translate into a lengthy period of time during which is difficult for Russia to acquire the expertise and investment needed to truly solve Y2K problems after they have gone through a period of "workarounds". In addition, it will, in all likelihood, delay and extend the time period Russia needs to become aware of Y2K-compliant computer technology from the west in the future.

In sum, I would anticipate that the effects of Y2K will linger far longer in Russia than they will in western countries that are better prepared on all levels to effectuate long-term solutions. In conclusion, while other countries no doubt will feel the economic effects of Russia's failure to prepare adequately for Y2K, sadly for Russia and its citizens, it itself will feel the brunt of the blow most dramatically. Ironically, given the heavy burdens that Russia already carries and the difficult life being led by its people today, it is not likely that Y2K will be identified as the source of the hardships. Rather, Russians will, in all likelihood, see little relationship between Y2K and their difficulties and will, accordingly, continue not to place a high priority on solving Y2K problems.

Mr. Chairman, thank you very much for affording the opportunity to join Professor McHenry and sharing my thoughts with you today.

[The prepared statement of Mr. Conn can be found in the appendix.]

Chairman BENNETT. Thank you very much for your insight. Let me ask you a totally personal question. The last time I was in Moscow, I dealt with Richard Werthlen of Latham and Watkins. Were you there on station the same time he was there?

Mr. CONN. Actually, Mr. Chairman, Mr. Werthlen, a good friend, came in to relieve me. I founded our office in 1991, end of 1991, and stayed there until Richard and his many children joined us in 1995.

Chairman BENNETT. OK. Well, he was very helpful on the issue that I was in Russia trying to deal with, and I am grateful to him and to Latham & Watkins for having him there. Is he still there?

Mr. CONN. Actually, he just recently left to return to Los Angeles. We have a new head of our office, one of my other partners, Sonia Golden.

Chairman BENNETT. Well, maybe it is a good sign for the long term that you keep office there. You assume that sooner or later Latham & Watkins will make some money out of Russia.

Mr. CONN. We would like to think that. We and all the other U.S. businesses over there tend to be a fairly hearty group that are ready for the rough roads.

Chairman BENNETT. For a long time.

Your testimony reminds me of a summary that we received on this committee. We sent two consultants to Russia, and to a number of countries around the world. They came back with their summary country by country, and the written summary, of course, was appropriately couched, but in the personal briefing, the lead consultant said to me, Nothing is going the work in Russia, and nobody is going to notice because nothing works now.

And that is kind of what I am hearing from the two of you. We could get into Chekov and Dosdieski and so on about their capacity for suffering. You have referred to that. But let us pick up on the comment about the connections with the rest of the world.

Gazprom not only provides natural gas for Russia but provides a very substantial amount of natural gas for western Europe. We can't get any answers as to what is going to happen in Russia beyond what I think the two of you have given us in your formal statement. But let us talk for just a minute about the impact a Y2K failure could have on eastern Europe and western Europe and other people who are more dependant on Russia for natural resources than, say, the United States is. Do either of you have a reaction to that?

Mr. MCHENRY. The only thing that I can say about that is that Gazprom has been working on the problem since at least the beginning of 1998, if not earlier, and now reports that only 7 percent of its systems are remaining to be remediated and also using a lot less computerization in general and is one of the richest organizations in Russia and has been installing SAPR–3, which is a major—it is called an enterprise resources planning package. It has been a similar solution adopted by a lot of western large multinational corporations to deal with their Y2K problem. So I am pretty hopeful about Gazprom and the fact that they are not going to have serious reductions in shipments.

I also say this: If anybody is going to reduce shipments because of Y2K, it will be inside the country. It won't be outside. So I am not seeing that as a significant threat. You might have a different opinion.

Mr. CONN. I would concur particularly with that final point that given desirability of raising hard currency, that it most likely would be domestic consumption within Russia that would be affected rather than foreign consumption, but we certainly have seen information indicating that—as you know, Gazprom is primarily involved in the transport of oil and gas, and we have seen information indicating that they do have many stations embedded with microprocessors that are located in Siberia and would have difficulty accessing those.

So I remain concerned that there will be interruptions, despite the fact that Gazprom certainly is well-capitalized at this stage.

Chairman BENNETT. So if there is—just to pick a number out of the air, if there is 25 percent loss in ability to produce and deliver, that will all come out of the Russians' hide, and the 75 percent that works will still be exported to the west.

Mr. CONN. I would think that would be tempered somewhat by the political pressures that would be brought to bear, but generally the pattern has been that oil exports, both legal and illegal depending on the regime in place at the time in Russia, have continued due to the market forces at work there, and I would expect that continue.

Mr. MCHENRY. Yes. No more comment.

Chairman BENNETT. You may not be the ones to ask this question of. I perhaps should have asked it to the previous panel, but given the amount of time that they had taken and my desire to get to this panel, I didn't want to prolong their being here.

The American news media has talked about "Moonlight Maze". This is a classified event, and so I have to be very careful about how much I talk about it publicly, but it has been identified in Newsweek and other sources as an attempt on the part of the Russians—they assume the Russians—to break into a variety of computers in the United States. And very recently, in the midst of Y2K and the lack of resources and the discussion of how much money they need from the west to help them, the prime minister recently signed an order authorizing—if I pronounce it correctly—Goskomtelekom to seek $50 million in credits to buy hardware and software in the west with the expected delivery in October or November.

It is hard to believe that that will go to Y2K remediation, but may be an attempt to increase—well, specifically they are saying they want to increase the number of Russian connections with the American internet and the amount of Russian involvement with the internet. That would suggest—and I don't want to go any farther than that because it is total conjecture, but that would suggest that their priority in the high-tech area has more to do with some kind of intelligence-gathering information with respect to American industry than it does with Y2K remediation and workarounds in their own society.

Do you have any reactions to that or comments about that? Is this just paranoia that is left over from the cold war that we need to put behind us? Or is this, indeed, another demonstration that the Russian leadership might be willing to allow their population to continue to suffer as they try to pursue some geo-political goal? You can answer better than the folks from the Government because you can speculate and they don't dare.

Mr. MCHENRY. Well, one thing I can say about that is that when this purchase was originally discussed in the press, at least back in July, the head of the State Committee on Telecommunications indicated that this might be a risky purchase for Russia because, in fact, Americans might try to embed intelligence-related functions in the computers that they would purchase. So I think that was a theme that was also struck by some of the military people who were setting up the joint early warning system.

So I think that there may be more paranoia or at least the same amount of paranoia on our side as there is on our side.

Chairman BENNETT. I have never underestimated the Russian capacity for paranoia.

Mr. MCHENRY. But by the same token, I do think that this represents a serious attempt to plug holes in critical systems because, as I have indicated in my writings, there are a certain number of old Soviet-era mainframe computers that are hanging around from the late 1980's that are in functions that would seem to need to be replaced, and I think that this funding may have more to do with replacing those and plugging some holes in critical systems than it does in increasing capacity to get to the internet.

So I would tend to think it is more not as serious a concern, but I would also say that any funding that we give them, any aid that we give them in this area, should be carefully monitored, just as we may have been or should have been doing in the past to see that it gets where it is supposedly going.

Mr. CONN. I would only add, although this is certainly far afield from the area that I normally focus upon, that in preparation for my testimony today, I certainly spoke with contacts in Russia regarding Y2K compliance issues and was struck by the amount of information that seemed to be coordinated by FAPSI and by the FSB, the successor to the KGB, which certainly, when you are dealing with Russia and Y2K and dealing with computers and technology, does take a leadership role.

Having said that, I would simply urge the same caution that my colleague mentioned in taking a close look at the transaction, but I would not have a view as to whether any level of paranoia is appropriate in this specific case.

Chairman BENNETT. OK. You talked of silver linings. One of the silver linings that we have found in this committee with respect to domestic situations is that some of the least prepared sectors of the economy, as they react to the Y2K challenge, are in fact making investments that they should have been making and were postponing. The original thought, which was that all Y2K expenses would simply be sunk costs and produce no return on investment, has given way to a recognition that, in fact, there will be some return on investment because of the modernization impact.

Can you comment on how much if any of that phenomenon will occur in the Russian activity?

Mr. MCHENRY. Yes. I think there is not going to be a very large silver lining effect of that at all in Russia, and the reason for that is the installation of new information systems has to go hand in hand with other parts of the economy that exist to support them, and there is a good reason why very little of the Russian economy is currently set up with just-in-time manufacturing or the kinds of real-time information exchanges that we fear will be destroyed by the Y2K bugs in the United States, and that is because the economy simply isn't functioning at that level of sophistication for the most part.

So I think, as my colleague said, at a certain time in the future when it becomes more attractive for investment that it will be necessary to invest in information systems along with the rest of the infrastructure and simply build whatever new industry is going to be built from scratch at that time. So investing in the information systems now, in fact, could be counterproductive in a lot of those

places except in supporting small businesses that, in my opinion, have already made that leap and are functioning on a capitalistic basis, which is largely in Moscow and St. Petersburg and just a few other places.

So I don't see much of a silver lining from that kind of investment. I do see the potential silver lining from increased contingency planning, from bringing the conditions that have been created that will go across ministry boundaries, may actually help the Russians to deal with some of the more severe problems in the future.

Mr. CONN. Yes. I could concur and just add that I think the opportunity here, the silver lining, is in the area of engagement that Senator Lugar spoke of as did the previous panel. Those opportunities certainly should be seized upon and built upon and make the best of obviously a difficult situation.

Chairman BENNETT. Thank you very much. I appreciate the outside kind of view that you give here that complements the inside bureaucratic view that we have had. Bureaucratic is not necessarily bad. That is why we have bureaucracies, to get us some of this information.

I am grateful and thank you again for your participation and your preparation. The committee stands adjourned.

[Whereupon, at 12:23 p.m., the committee was adjourned.]

APPENDIX

ALPHABETICAL LISTING AND MATERIAL SUBMITTED

PREPARED STATEMENT OF KENNETH BAKER

Thank you Mr. Chairman and members of this Committee for the opportunity to appear before you today to present this statement for the record on the Department of Energy's activities to address the year 2000 (Y2K) computer problems of Soviet-designed nuclear power reactors.

I commend the work this Committee is doing to highlight the importance of the year 2000 issue in both the United States and internationally. I look forward to working closely with this Committee, particularly as it relates to the 68 Soviet-designed power reactors located in the New Independent States (NIS) and in Eastern European Countries. Today, I will briefly review our ongoing activities to improve the safety of Soviet-designed nuclear power reactors to provide you the context for today's year 2000 discussion. I will then discuss our understanding of year 2000 problems that exist at these plants and review the actions we have already taken to assist in reducing the risk of an accident. Finally, I will describe our path forward through the end of this year.

AT the outset, however, I wish to emphasize that the Department is providing assistance to countries, not managing their Y2K remediation efforts. The Department's experts have held many meetings with the host country's experts and visited several of their nuclear power plants to evaluate their Y2K needs. Although some Soviet-designed nuclear power plants continue to be at higher risk of a nuclear accident due to difficulties in design and operating conditions, based on our current information and the ongoing Y2K-related work being done at the nuclear facilities, we conclude that there is not a significantly increased risk of a nuclear accident due to a Y2K event. The Department's experts expect the primary safety systems to continue to function properly to shut down the plants safely, if needed, during a Y2K event. However, there are Y2K issues with other systems important to safety and normal plant operations that, if left uncorrected, could compromise nuclear safety. We are continuing to work with the host countries to address these issues.

Ongoing Activities to Improve Safety

The 1986 disaster at the Chornobyl nuclear power plant revealed many flaws in the Soviet approach to nuclear power. The reactors and nuclear infrastructures left behind by the Soviet government continue to operate in nine countries. These reactors, including one that still operates at the Chornobyl site, suffer from deficiencies in training, safety procedures, design, and equipment. Some problems have been exacerbated by the breakup of the Soviet Union—equipment shortages are commonplace and many nuclear professionals suffer from low or erratic pay. If not corrected, these conditions pose a continued risk of a reactor accident in Ukraine, Russia, Armenia, Kazakhstan, Lithuania, Slovakia, Czech Republic, Hungary, and Bulgaria. The current year 2000 concerns are only a portion of our continuing concerns.

If another major nuclear accident occurred, the United States and the international community would be forced to deal with the political, economic and environmental destabilization of politically sensitive regions. This concern led the U.S. Government to conclude that enhancing the safety of Soviet-era nuclear reactors and establishing improved safety infrastructures in the countries that operate them is a vital national security interest of the United States. The U.S. and other Western countries have the technologies and skills to work with these nations to address nuclear safety challenges with a relatively modest investment. Rather than providing billions of dollars in foreign aid to correct all of the problems directly, the safety program helps the host countries structure their nuclear industry to address safety issues, to prevent accidents, and, as their economies improve, to increase

their own funding for nuclear safety. These activities are critical to preserving these emerging, democratic, free market economies.

I am proud of the progress the Department of Energy has made to improve the safety of Soviet-designed nuclear power plants and in establishing self-sustaining nuclear safety infrastructures in these countries. The Department is working with the host countries and the personnel at all 68 nuclear power reactors, which are located at 23 sites. There are several different designs, including the RBMK, or Chornobyl-type, the VVER–440 and the VVER–1000. The greatest safety concerns pertain to the RBMK and early models of the VVER–440. We are addressing the most serious risks at these reactors by improving the plants' physical operating conditions, installing safety equipment, developing improved safety procedures, establishing regional centers for training reactor personnel, and conducting in-depth safety assessments of the operating plants.

Some understanding of the actual risk can be achieved based on recently completed probabilistic risk assessments performed by international experts at two RBMK plants; one at the Ignalina plant in Lithuania and another at the Leningrad plant in Russia. Regardless of the year 2000 situation, if no safety upgrades were performed, risk experts calculate that the frequency of a core meltdown accident at an RBMK reactor is approximately one-hundred times higher than at a typical U.S. nuclear power plant.

Unlike U.S. plants, RBMK reactors do not have containment structures, making the consequences of a core meltdown even more severe.

The Department is also working to convert the operating modes of the three nuclear production reactors located at Seversk and Zhelenogorsk in Russia to enable the reactors to continue operations without producing weapons grade plutonium. These plants are old and have some of the same serious safety issues associated with RBMKs.

Accomplishments of the Department's program range from installation of safety parameter display systems at the Chornobyl plant in Ukraine and the Kursk plant in Russia, to completing training for thousands of reactor staff at the Balakovo training center in Russia and the Khmelnytskyy training center in Ukraine. Equipment, such as pipe lathe and welding equipment, firedoors, back-up generators, dry cask spent fuel storage systems and additional safety equipment and materials, has been delivered to plants throughout the former Soviet Union. The list of accomplishments to date is extensive, and the equipment and other activities are having very positive impacts on the safety of operations at these plants.

The Year 2000 Problem at Soviet-Designed Nuclear Power Plants

The U.S. Department of Energy is working closely with the International Atomic Energy Agency (IAEA) to help resolve year 2000 (Y2K) issues associated with Soviet-designed reactors. The Department has received requests from Russia, Ukraine and other countries for Y2K assistance in the nuclear power sector. The Department is responding to these requests by assisting these countries in their efforts to address safety-related Y2K issues at their reactors. Let me briefly state the objectives of our Y2K initiative for Soviet-designed reactors and outline our accomplishments thus far. Then, I will summarize the current status of the ongoing work and the path forward.

Purpose and Objectives

the goal of the Department's program is to assist countries with Soviet-designed reactors address safety-related Y2K issues. We are helping to ensure that Y2K events will not cause an accident or significant challenge to plant safety. We have been working in cooperation with the host countries since 1998.

Accomplishments

Most of the contributions we made early on were in the form of workshops and training, sometimes bilaterally with the host country, at other times in conjunction with the International Atomic Energy Agency (IAEA). The IAEA has developed guidance for conducting Y2K evaluations at nuclear power plants based on the Nuclear Energy Institute Y2K assessment guidelines used in the United States. The Department initially conducted an October 1998 workshop in Moscow on Y2K issues for nuclear power plants in Russia. This workshop was hosted by the Russian utility that manages nuclear power plants, Rosenergoatom. A similar workshop was conducted in March 1998 in Kyiv, Ukraine. This workshop was hosted by the utility responsible for Ikraine's nuclear plants, Energoatom.

We supported a training workshop on the IAEA's Y2K Guidance Document for member countries in Vienna, Austria on January 25 through 29, 1999. The guidance helps to standardize the efforts across all the nuclear power plants. We sponsored the development of software to assist plants with using the IAEA Y2K Guidance and in sharing information gathered via the Internet.

Transmission and distribution of electric power is another significant Y2K issue. We conducted Transmission and Distribution Year 2000 Information Exchange Workshops in Moscow, Russia in February 1999 and in Kyiv, Ukraine in March 1999 to assess current Y2K programs within the Russian and Ukrainian transmission and distribution systems.

To assist in implementing the IAEA guidance, we sponsored the development of draft procedures to conduct an IAEA Y2K Guidance-based assessment process.

To gain a plant perspective of how the Y2K assessments were going, we participated in Russian reviews of the ongoing Y2K evaluation work at the Beloyarsk and Kola nuclear power plants. In addition, we have visited the Leningrad, Chornobyl, Zaporizhzhya, and Armenian nuclear power plants and have met with representatives from almost all the Soviet-designed reactor facilities during meetings in Moscow, Kyiv, Vienna, and the U.S.

A technique that proved valuable in our other safety work was arranging visits to U.S. nuclear plants to observe how US plant managers dealt with specific issues. In this instance, we sponsored visits in July to the Surry and Calvert Cliffs plants for Russian Y2K specialists and the San Onofre and Palo Verde for Ukrainian representatives. During the visits, they reviewed U.S. Y2K assessments, the remediation work completed, and the process of developing contingency plans. Part of the team was made up of Y2K specialists from the Russian and Ukrainian nuclear regulatory organizations.

Also in July, we supported an IAEA Information Exchange Workshop for member countries in Vienna. This provided an opportunity for discussions of the ongoing Y2K work in each country.

The week of July 26, we sponsored the training of Russian, Ukrainian, and Lithuanian personnel in automated software scanning tools. Such tools can much more rapidly and accurately scan lines of computer codes than laborious manual reviews during assessment and remediation efforts. The Department has provided a countrywide license for this tool for use at nuclear plants and transmission and distribution centers throughout Ukraine. The Department also provided funding to Ukraine for the computers and personnel to operate the software. These actions will improve the manual process that was being used in Ukraine to review and change the date-sensitive parts of the computer programs. Software licenses for the scanning tools also were provided for both units at Ignalina plant in Lithuania.

Summary of Our Current Knowledge of the Situation

I am pleased to say that initial complacency in some countries with Soviet-designed nuclear plants has greatly improved. Although some Y2K response efforts were only begun within the last year, significant progress is now being made. Most of the host countries are following the IAEA guidance closely when conducting Y2K assessments of their nuclear plants and electrical transmission and distribution facilities.

Equipment provided by the United States has been carefully evaluated for Y2K safety concerns. This evaluation and follow-up remediation has ensured that no equipment provided by the United States will cause a Y2K safety problem.

Based on recent information, Russia, Ukraine and other host countries have established adequate Y2K programs. We have categorized their programs into four phases. Phase one is inventory/preliminary assessments; phase two is detailed assessment/testing; phase three is remediation; phase four is contingency planning. Of the 68 nuclear reactor units in the nine countries of the former Soviet Union, 50 have completed their phase two detailed assessments and testing activities. Each of the 50 is underway with its phase three remediation activities. The remaining nuclear units are proceeding to complete their detailed assessments and testing activities. Of the total, 45 have begun developing their phase four contingency plans.

Our understanding of each country's Y2K program for its nuclear power plants is shown in the attached Table, "Summary of Y2K Compliance at Soviet-Designed Reactors, September 1999."

While much work remains to be done, let me emphasize that current information indicates that there are no known Y2K problems with the primary reactor safety systems. These systems detect problems and automatically shut down the plant. Therefore, if something goes wrong at the plant, we expect that the primary safety system will continue to function properly and shut down the plant safely.

Not all the countries are at the same stage of readiness, however, Russia has established a well-organized and aggressive, if under-funded, Y2K program. Each plant has reported that it has completed its preliminary and detailed assessments, although the depth and accuracy of these assessments are not completely known by us. The nuclear power plants in Russia plan to complete remediating their important systems in October 1999. On the other hand, Ukraine has developed an assessment plan, but until lately had only completed limited assessments. The Depart-

ment of Energy is partnering with the Science and Technology Center in Ukraine to work with the Ukrainian utility and nuclear power plants to conduct systematically a slightly varied implementation of the methodology described in the IAEA Y2K Guidance document. Ukraine plans to complete its remediation activities by November 1999.

There are Y2K safety concerns with nuclear power plants in Russia and Ukraine. Specifically, systems without direct safety impact, but that are important to safety, have known Y2K problems. Common to both RBMK and VVER reactors are monitoring computers, such as the plant process computer. This computer monitors conditions within the reactor and provides information to the operator. The operator uses this information to make various adjustments to the plant, such as moving control rods or changing flow rates. Failure of the plant process computer is not an immediate safety concern, but regulations require that the plant be shut down within a few hours or less, if the computer is not restored to full operation. RBMK plant process computers are known to suffer from both hardware and software Y2K vulnerabilities, while at VVERs problems are generally confined to software issues.

The radiation monitoring system, which is a system important to safety, is another system at Soviet-designed reactors with known Y2K vulnerabilities. The operator of the nuclear facility would be required to shut down the reactor if it failed. The security access system, which allows personnel access to parts of the nuclear plant to check on the performance of equipment and instruments, is also known to have Y2K vulnerabilities. Other systems that are Y2K vulnerable, for example, are the ancillary systems connected to the plant process computer to calculate the state of the reactor core. The core monitoring software that calculates the power distribution in the nuclear core and the fuel management system that calculates the nuclear fuel that is burned are also Y2K vulnerable. Failure of each would require the operator to shut down the reactor.

There is concern that, if not fixed, these problems could result in the simultaneous shut down of several nuclear plants, causing disruption of power supplies in the middle of winter. In 1997, the nuclear power plants in Russia produced 14 percent of the nation's electricity; in the far western parts of Russia, the share was nearly 25 percent. The Kola, Leningrad, and Smolensk nuclear power plants supply half of northwest Russia's electricity requirements. In 1997, Ukrainian nuclear power plants produced 47 percent of the nation's electricity. Thus, shutting down these reactors could have a serious impact on the populace. Alternatively, there may be pressure to keep the plants running, even without the plant process or other monitoring computers, which would then create a safety problem. In general, the Russians report that they have remediated their plant process computer software vulnerabilities using a manual review process. Work is in progress in Ukraine to remediate these same problems using tools provided by the Department.

Moreover, the following Y2K safety concern exists in all the host countries. Y2K problems may originate within the electrical transmission and distribution system and cause an unplanned reactor shut down (referred to as a loss of off-site power accident).

Russian and Ukrainian transmission and distribution experts have stated that they have found Y2K problems with their automated systems; however, they are confident that they can operate their systems in a manual code and avoid any unplanned disruption of electricity supplies to the nuclear power plants. The situation in the other host countries is expected to be similar. Host-country experts are more concerned that Y2K would cause the nuclear power plants to shut down which would in turn cause disruption of electric supplies. Any unplanned shut down due to a loss of off-site power poses risks to the safety of the nuclear power plants, because emergency battery and diesel power systems must function properly to ensure plant safety.

The Department has discussed with Russian and Ukrainian government officials the importance fur sufficient supplies of diesel fuel to power the back-up electrical generators, if there were a loss of off-site power event caused by Y2K. Our experts also are meeting with the nuclear power plant staffs to better assess the adequacy of diesel fuel supplies.

The host countries in conjunction with the Department of Energy are working to develop contingency plans to address these Y2K concerns. These plans help plant operators understand possible Y2K problems that may occur and establish procedures to address potential problems. The plans would help prevent operators from inadvertently creating a worse situation due to inappropriate operator actions.

Path Forward

Based on meetings at the IAEA and discussions with the host countries, the countries of Bulgaria, Czech Republic, Hungary, Lithuania, and Slovakia appear to be adequately addressing Y2K issues. Kazakhstan has permanently shut down its

BN350 reactor, limiting Y2K assistance to equipment for monitoring the plant during shut down and its spent fuel. Therefore, the Department is focusing its assistance in the countries of Armenia, Russia and Ukraine, with limited assistance to Kazakhstan.

In most countries, the preliminary and detailed assessments are complete or are nearly complete. In Russia, the Department's efforts complement the efforts of the International Science and Technology Center. The Center is pursuing a program at Russian nuclear power plants to help verify the preliminary and detailed Y2K assessments that the Russian nuclear power plants had completed before using systematic guidelines. The Center plants to complete those assessments that are either deficient or incomplete according to their established Y2K guidelines. The Russian utility, Rosenergoatom, provides the results of the assessments sponsored by the Center directly to the Department which in turn develops a Y2K remediation assistance strategy for the nuclear power plants. The Department's remediation assistance complements the existing Y2K programs at the nuclear power plants.

In addition, the Department has participated in two Russian reviews of the Y2K evaluations conducted at Russian nuclear power plants. These reviews were held at the Beloyarsk and Kola plants. The Department experts will also participate in a review at the Bilibino plant (near Alaska) in mid-October.

Similarly in Ukraine, efforts will continue under the partnership with the Science and Technology Center in Ukraine, Ukrainian institutes, and nuclear power plants to implement, with slight variances, the IAEA Y2K guidance at all the plants. This will complement the work already completed with the IAEA's help at Chornobyl Unit 3, Zaporizhzhya Unit 6, and South Ukraine Unit 3. The Department works closely with the IAEA during its ongoing reviews of the assessment efforts in the host-countries.

The Department is providing assistance in remediating identified Y2K problems in Russia, Ukraine, Kazakhstan and Armenia. Because of the assessment efforts, specific problems have been identified and the plants have requested assistance to remediate these problems. In Russia, the utility and nuclear power plants have requested assistance in purchasing replacement hardware and software for systems that will be important in maintaining continued operations. Similar requests have been received from the Chornobyl and Zaporizhzhya nuclear power plants in Ukraine and the nuclear power plants in Kazakhstan and Armenia. Efforts are underway to provide these requested materials and assistance. In addition, it is expected that the rest of the nuclear power plants will also have similar requests as their detailed assessment work progresses. When these additional deficiencies are discovered and prioritized at other plants, consideration will be given to providing assistance to correct the deficiencies.

Regarding the reliability of the electrical transmission and distribution systems and their impacts on nuclear safety, this issue is being addressed primarily by the development of Y2K contingency plans. The Department sponsored a contingency planning workshop during the week of September 19, 1999 in Prague for Armenian, Bulgarian, Czech Republic, Hungarian, Lithuanian, and Slovakian nuclear power plant and transmission and distribution personnel. Similar contingency planning working sessions are scheduled this week in Russia and in October for Ukraine. The working meetings are intended to assist the plants and utilities of the host countries in completing their contingency planning. These meetings are being coordinated with similar International Energy Agency meetings in Paris and Prague in late September and early October. Personnel from U.S. plants and utilities will attend in order to share their contingency plans and experiences. In addition, Ukrainian and Russian representatives visited the United States earlier this month to observe the nationwide North American Electric Reliability Council year 2000 drill on September 9, 1999.

The Department is coordinating with the U.S. Nuclear Regulatory Commission to provide assistance to host-country regulatory bodies as requested. The nuclear regulatory bodies in the host-countries have participated in meetings with the Department's experts. They have advised the Department's experts, based on information obtained from IAEA meetings and visits to the U.S., on Y2K issues related to their regulations. The regulatory body in Russia, for example, was a major contributor to the development of the Russian version of the IAEA Y2K guidance document.

Conclusion

We are relying on the host countries to assess their Y2K issues properly, remediate problems, and develop contingency plans using established guidelines. We have provided information and assistance at each step along the path to Y2K readiness. The initial complacency that was expressed by some host country representatives has given way to significant efforts on their part to resolve Y2K problems. In light of the relatively late start of these Y2K activities, we cannot be completely cer-

tain that they will be successful. On the other hand, as I stated earlier, we do not anticipate failure of primary safety systems. Therefore, the Department's experts believe that there is not a significantly increased risk of a nuclear accident at Soviet-designed nuclear power plants due to a Y2K event. We are helping to remediate the monitoring systems, such as the process computers, which if they failed should lead to an orderly shut down of a plant according to safety procedures. We are providing assistance with contingency planning and will continue to work toward resolution of Y2K issues at Soviet-designed nuclear power plants.

Nonetheless, some known Y2K problems that do not directly affect plant safety or continued operation of the plant probably will not be corrected before the end of 1999.

Table. Summary of Y2K Compliance at Soviet-Designed Reactors, September 1999

Country (9)	Plants (23)	Type	Sub-Type	Number of Units (68)	Systematic Y2K Methodology In Use	Inventory/Preliminary Assessment Complete	Detailed Assessment /Testing Complete	Remediation Complete	Contingency Planning Complete
Armenia	Armenia	VVER	440/230	1	Yes	Udwy	Udwy	Udwy	Udwy
Bulgaria	Kozloduy	VVER	440/230	4	Yes	Yes	Yes	Udwy	Udwy
Bulgaria	Kozloduy	VVER	1000	2					
Czech	Dukovany	VVER	440/213	4	Yes	Yes	Yes	Udwy	Udwy
Hungary	Paks	VVER	440/213	4	Yes	Yes	Udwy	Udwy	Udwy
Kazakhstan	Aktau	BN	360	1	No[1]	Yes[1]	Yes[1]	Udwy[1]	
Lithuania	Ignalina	RBMK	1500	2	Yes	Yes	Udwy	Udwy	Udwy
Russia	Kola	VVER	440/230	2	Yes[2]	Yes	Yes	Udwy	Udwy
Russia	Kola	VVER	440/213	2					
Russia	Leningrad	RBMK	1000	4	Yes[2]	Yes	Yes	Udwy	Udwy
Russia	Smolensk	RBMK	1000	3	Yes[2]	Yes	Yes	Udwy	Udwy
Russia	Kursk	RBMK	1000	4	Yes[2]	Yes	Yes	Udwy	Udwy
Russia	Bilibino	LGWR	12	4	Yes[2]	Yes	Yes	Udwy	Udwy
Russia	Kalinin	VVER	1000	2	Yes[2]	Yes	Yes	Udwy	Udwy
Russia	Novovoronezh	VVER	440/230	2	Yes[2]	Yes	Yes	Udwy	Udwy
Russia	Novovoronezh	VVER	1000	1					
Russia	Beloyarsk	BN	630	1	Yes[2]	Yes	Yes	Udwy	Udwy
Russia	Balakovo	VVER	1000	4	Yes[2]	Yes	Yes	Udwy	Udwy
Russia	Seversk	ADE		2	Yes[3]	Udwy	Udwy		
Russia	Zhelenogorgsk	ADE		1	Yes[3]	Udwy	Udwy		
Slovakia	Bohunice	VVER	440/230	2	Yes	Yes	Udwy	Udwy	Udwy
Slovakia	Bohunice	VVER	440/213	2					
Ukraine	Chornobyl	RBMK	1000	1	Yes[3]	Yes	Udwy	Udwy	Udwy
Ukraine	Rivne	VVER	440/213	2	Yes[3]	Udwy	Udwy	Udwy	Udwy
Ukraine	Rivne	VVER	1000	1					
Ukraine	Khmelnytskyy	VVER	1000	1	Yes[3]	Udwy	Udwy	Udwy	Udwy
Ukraine	Zaporizhzhya	VVER	1000	6	Yes[3]	Udwy	Udwy	Udwy	Udwy
Ukraine	South Ukraine	VVER	1000	3	Yes[3]	Udwy	Udwy	Udwy	Udwy

(Udwy = Underway/in progress)

[1]Aktau NPP has been shut down and will not be restarted. Staff members report that they have reviewed their remaining operating systems for Y2K issues and require some assistance in remediation.
[2]Minatom and REA report that all commercial NPPs in Russia are employing a methodology based on the IAEA's Y2K Guidance. REA has reported that all commercial NPPs in Russia have completed their inventories and preliminary assessments and are proceeding with detailed assessments and testing.
[3]Energoatom has agreed to work with STCU and OSI to implement a Y2K program based on the IAEA's Y2K Guidance at all its NPPs.

PREPARED STATEMENT OF CHAIRMAN ROBERT F. BENNETT

A serious social, economic, and political crisis began when Russia devalued the ruble and defaulted on its debts in August 1998. Little work has been done to investigate the long-term consequences Y2K could bring to a Russia already on the edge. This troubles the Committee, since Y2K failures in key infrastructures such as

PREPARED STATEMENT OF CHAIRMAN ROBERT F. BENNETT

A serious social, economic, and political crisis began when Russia devalued the ruble and defaulted on its debts in August 1998. Little work has been done to investigate the long-term consequences Y2K could bring to a Russia already on the edge. This troubles the Committee, since Y2K failures in key infrastructures such as

power, banking, telecommunications, and defense might have serious negative impacts on the stability of the Russian economy and political environment.

The International Monetary Fund (IMF) announced on Friday that it would offer special loans to countries suffering serious economic damage from Y2K. The IMF certainly hopes this financial assistance won't be needed, but states, "there are uncertainties, and the potential consequences for international trade and growth of possible interruptions to productions and shipment may be significant." I think these uncertainties and the potential consequences resulting from Y2K apply as much to Russia as to any nation.

While Russia is not as highly networked and interconnected as the United States, it still relies on information systems and microchips. In fact, the information systems that survived the Soviet era and remain in use are extremely critical. As many as 4,000 Soviet-era mainframes are estimated to support the operation of Russia's industrial and defense enterprises. It is believed that several hundred million dollars is needed to repair these mainframes. The failure, disruption, or corruption of these systems in a short span of time could create a unique and unexpected challenge to the economy. In the short term, the shock from serious Y2K failures could exacerbate Russia's downward economic spiral. Since such an event would unquestionably affect U.S. policy, we must proactively consider how we should respond to these failures if and when they occur.

From a long-term perspective, no one knows what the impact of Y2K inefficiencies will mean for the Russian economy as a whole. We must decide soon what our foreign policy will be with respect to Y2K failures. We cannot engage in diplomatic shell games until November 1999 and then glibly announce "The U.S. Foreign Policy on Y2K." What's more, I fear that whatever policy the White House has arrived at will crumble when the first CNN footage hits the air. What should U.S. policy be with respect to foreign Y2K failures? How will we prioritize national security, the needs of our allies, the needs of critical trading partners, and humanitarian needs? These will be very difficult decisions and there will be no time for "spinning' rhetoric and political posturing. Difficult decisions will demand prompt and careful attention. The U.S. does not have the resources to save the world. Indeed, if it weren't for the fast actions of Senator Stevens, we might not have had the emergency funds to meet emergency requirements here at home.

It is vital to remember that Y2K problems will unfold over time. We here in Washington have expended a lot of effort to examine the immediate impact of Y2K—from sharing nuclear information to collecting information about telecommunications—but we've given little consideration to what happens if and when problems emerge in late January or in March.

Since the dissolution of the Soviet Union, America has reached out to try and help the Russian Federation wherever it was prudent to do so. We are most fortunate to have one of the Senate's foremost Russian experts—and a valuable Committee member—with us today. In 1991, Senator Lugar recognized the urgent need to help Russia move its nuclear and chemical weapons back within its sovereign borders. Through Cooperative Threat Reduction, the U.S. and Russia collaborated to dismantle launchers and destroy chemical weapons in the newly independent states. It is precisely because of this expertise that we have invited him here today to share his thoughts about how assisting the Russians with Y2K fits into the broad goals of threat reduction.

PREPARED STATEMENT OF JOHN R. BEYRLE

Thank you, Mr. Chairman and members of the Committee. I am pleased to have the opportunity to discuss the potential impacts and consequences for the Russian Federation of the Year 2000 computer problem. That the focus of this hearing is solely on Russia and Y2K is evidence of the justifiable concern of the Congress and the American people on what the potential for disruption associated with the millennial change may mean for our national security. Addressing potential problems connected with Russia's strategic arsenal and safety questions raised by its aging nuclear power infrastructure has been the priority focus of our engagement with Russian officials and agencies: concern for our own well-being would dictate nothing less. Accordingly, Assistant Secretary of Defense Warner is prepared to brief you on our efforts to continue and enhance cooperation in the areas of nuclear weapon security, the sharing of missile launch data, and in ensuring open communications among our leaders during the Y2K transition. And my colleague Ken Baker, Deputy Assistant of Energy, will be discussing his Department's efforts to ensure that Russia's many nuclear power plants are not adversely disrupted during Y2K.

I would like to open our discussion today by providing a brief overview, from the perspective of the Department of State, of our current assessment of some of Russia's Y2K preparations. It seems easy to predict Russian difficulties resulting from the possible effects of Y2K. The country is only slowly recovering from the financial collapse it suffered over a year ago, a situation which inevitably distracted the government from its efforts to deal with potential Y2K disruptions and left less in the budget for remediation efforts. Frequent changes at the top of the Russian government over the past year have further complicated the picture. Moreover, by the first of January Russia will be experiencing a transitional political situation. A new Duma will have just been elected, and presidential elections will be just a few months off.

I would like to emphasize from the start that our assessment of Russia's vulnerability to Y2K is an ongoing, iterative process. We have been and remain continually engaged with the Russian government at a variety of levels in a range of areas in an effort to gather the information we need to make definitive assessments in the areas of greatest concern or most direct impact on American interests. In general, the amount and quality of information available, while not optimal, has been sufficient for us to make evaluative judgments in these key areas—judgments that we are continually reassessing or refining as the situation on the ground changes, or new data become available. But as this Committee knows all too well, the Year 2000 technology problem is without precedent in history, and uncertainty attends all of our efforts to deal with it. With regard to Russia especially, the challenge lies in assessing how this uncertainty translates into risk. We do not underestimate the potential disruptions that Y2K may bring to Russia, but at the same time we need to evaluate such problems realistically.

Russia's success in navigating the Y2K transition throughout its society rests in large part on its ability to minimize electricity and communications disruptions, and thus I would like to concentrate this overview on our analysis of the electrical and telecommunications sectors. Russia is likely to experience disruptions in its electrical grid and telecommunications infrastructure, with subsequent effects on its financial, industrial, and government sectors. At this time we do not foresee severe, long-term disruptions. Our analysis of Russia's electricity sector indicates the larger cities, Moscow in particular, are likely to be much less affected by outages than the countryside. Depending on how effective the authorities' Y2K remediation efforts are in the three remaining months, it appears that Moscow and the other cities might emerge relatively unscathed by the transition.

We attribute this partially to the Russian government's traditional concern and attention to the urban populations, dating back many decades. In fact, as we understand the electrical sector priorities, power to the countryside might be reduced in order to ensure that the cities are not deprived. If the overall integrated power system (IPS) is not fully functional, this could result in power deficits, perhaps lasting several days, to the smaller towns and villages.

The power utilities' ability to supply electricity will likely vary from region to region. The Far East, for example, will likely face the greatest risk of power loss or shortages. On the other hand, because of the economic contraction of the past decade, many areas are currently using much less power than previously. Coupled with the extended holiday period, which decreases electricity demand, this should result in significant excess generation capacity. This in turn should reduce the stress on the electrical grid, and provide more flexibility to the power generation and distribution operators to work around problems that may develop in individual plants.

Russia presently derives seventy percent of its power from fossil fuel plants, mostly natural gas; fifteen percent from hydropower; and fifteen percent from nuclear plants. With respect to the non-nuclear plants, we understand that many of them use older, analog systems that should not be affected by the Y2K rollover. We are still collecting information on how many of these plants have been upgraded with more modern plant process controllers, which could have non-compliant embedded microprocessors.

With respect to the nuclear plants, my colleague Ken Baker from DOE can provide you with more information about the dedicated Y2K programs that his organization has undertaken, and their cooperative efforts with the IAEA and the U.S.-supported International Science and Technology Center.

It is no secret that Russian winters are cold. Any disruption of the heating systems in Russia could have serious, potentially life-threatening consequences. The reliability of the heating systems is tied closely to the availability of electricity. In larger cities such as Moscow, heat is provided mostly by natural gas-operated water heating plants, while coal-fired plants are more common in the small cities and towns. The plants are analog and should not be affected by Y2K, but once again, electricity is required to pump the water through the pipes and return it.

A somewhat greater potential for disruption, in our view, lies with the Russian telecommunications sector. There are two to three thousand domestic telephone companies around the country. They use a wide variety of equipment, produced both domestically and abroad. We believe some of that equipment contains embedded microprocessors that are not Y2K-compliant. The consequence of this is that some of the systems will likely fail, disrupting normal telecommunications services. It could take the telecommunications companies days and perhaps weeks to track down and repair all the failures.

Russia has access to updated telecommunications satellites, which we believe to be Y2K-compliant. Less clear is the status of ground-based links, some of which may rely on embedded chips. Cellular systems are also up-to-date but they too frequently rely on landlines to relay conversations beyond the local cell. The government and telecom providers are working to minimize disruptions, but we doubt that they have sufficient time or money to resolve all problems in time.

Many vital industries and government entities have one or more backup communications system. We believe the Soviet-era internal phone system that connects many government ministries and agencies should continue to function. The electricity monopoly, UES, has its own communications system using power lines, as well as other backup systems. Key energy players like Gazprom, Transneft, Transgas, and RosEnergoAtom, also have one or more backup systems. It is not clear that the backup systems are entirely reliable, but having doubly redundant backups provides some measure of security in these key sectors.

Regarding air traffic safety, we understand that national systems such as the Moscow area control center, the Rostov air traffic control center, the data transmission system, and the automated planning system on airspace use, have all undergone extensive Y2K testing. Potential Y2K problems have been or soon will be corrected. Russia's national aviation authority requires that regional air traffic control centers test their equipment and implement contingency plans in case of Y2K disruptions; most of these centers have complied, and the remaining few are expected to do shortly. In addition, the authority will order the grounding of any aircraft that has not provided a statement of Y2K compliance by December 1.

Given the efforts that Russia has made in remediating potential Y2K disruptions and in making contingency plans, at this time we are hopeful that we will not need to reduce staff in our embassy and three consulates in Russia. We expect to make a final determination in mid-October. Nevertheless, we are advising U.S. citizens who will be in Russia over the millennial transition to be prepared for possible disruptions, especially in key sectors like electricity, heat, and telecommunications. As always, we strongly urge all U.S. citizens to register at one of our missions and to remain in contact for updated information.

The U.S. has worked closely with key sectors in Russia to prepare for the transition. We have focused particularly on those areas related to national security, as my colleagues will relate. For example, in the nuclear safety area, the Energy Department began an active program a year ago, which has been well received in Russia.

In addition, however, thanks to funds appropriated for this purpose by Congress, we have carried out a number of activities with and inside Russia. Beginning earlier this year we cooperated with the Russian Government, the World Bank, the International Energy Agency (IEA) and the American Chamber of Commerce in Russia to conduct a series of workshops and seminars in Russia on the Y2K issue. We have sent U.S. experts to Russia and have funded the travel of Russian experts to various international meetings and conferences. We have also conducted videoconferences between U.S. and Russian officials and opinion leaders to increase awareness of Y2K issues.

In these outreach efforts, we have tended to focus on those government agencies that provide key services. For example, two groups of mid-level Russian government officials have visited the U.S. in the past year under the USIA international visitors' program to discuss preparations for Y2K at the sectoral level. We are preparing another group of Russians to visit the U.S. under the same program to look at how U.S. utilities prepare contingency plans for Y2K. The State Department, USIA, and the Department of Commerce also co-sponsored two conferences in Russia for small and medium enterprises. Hundreds of Russian-language CD-ROMs to assist these businesses in making Y2K contingency plans were distributed at these conferences. USIA has also developed a Russian-language website.

Our efforts and those of the world press have heightened awareness of the problem in Russia. The Russian Government published a plan for tackling Y2K as early as May 1998. Moscow's efforts have been hampered by lack of money, however. Since the August 1998 economic crisis in particular, there have been insufficient funds to deal with known problems.

Our experience in attempting to help, or even in obtaining information on the extent of the problem in some sectors, has been mixed. Some agencies, such as the electricity monopoly United Energy Systems, have been open to technical exchanges with Western experts. But for much of the Russian government transparency still comes hard.

Some in the Russian bureaucracy view Y2K as a national security issue and are reluctant to reveal any information that could betray weakness or vulnerability. This reticence has hundreds of years of tradition behind it, but makes it more difficult for Russian interagency remedial work, and definitely more difficult for foreigners to assess the problem accurately. To illustrate, one key ministry refused to meet with U.S. Embassy officials to discuss their Y2K preparations because they did not want to "spread rumors."

This reluctance also complicates our ability to forecast accurately what additional steps might be necessary to protect Americans living and working in Russia. We have posed a number of questions to the Russian authorities concerning basic service during the transition but have received few answers. Some of these lists of questions were put to them as long ago as June. We will continue to seek satisfactory answers on behalf of the many Americans who live in or do business with Russia.

In conclusion, Mr. Chairman, please allow me to make a few general points.

First, in assessing Russia's overall vulnerability, it's important to bear in mind that much of the country's infrastructure is less dependent on computer technology than in some Western countries. This fact tends to lessen the risk of large-scale, systemic failures—the kind that are more complicated and take longer to repair—in favor of more localized problems that can be fixed more easily and quickly. Unfortunately, it has also led to a certain complacency on the part of some in the government and financial community and a tendency to understate the actual risk potential.

Second, the level of technical and engineering expertise in ratio to the problems anticipated is relatively high. Programmers and engineers are at work on remediation efforts now, and are prepared to deal with the shocks and aftershocks as the millennium rolls over. Schooled in the communist era of shortages, when the unavailability of replacement systems meant fixing and re-fixing, they have been compelled to become intimately familiar with their systems, and can be creative and resourceful in dealing with novel or unanticipated problems. But it's important to remember that Y2K is an unprecedented problem of potentially large-scale magnitude. Even with the best will and capabilities, there may be too many problems to deal with, requiring prioritization of the effort. Furthermore, it is far from clear that Russia will have sufficient resources to deal effectively with the consequences.

Third, many elements of the Russian Government are working diligently to prevent disruptions in the key electrical sector, and in other areas that my colleagues will discuss. Most Russians recognize that this problem is not hypothetical. They do not have their heads in the sand, but they are struggling to do what is needed as the clock ticks down. In our assessment, as I have mentioned, the failures are not likely to be severe or long lasting. If that is the case, then we should not expect significant economic fallout. However, the Russian Government has stated that certain financial resources—estimates vary widely—will be necessary to upgrade or replace deficient equipment. DOE, IAEA, and ISTC are helping provide this equipment in the nuclear area, and Dr. Warner will discuss the potential for similar assistance in DOD programs. To date, Russia has neither asked for nor received significant aid in other Y2K problem areas. This means Russia must allocate the money internally, a difficult process in their current financial situation. If the resources are not made available, they would likely fall short of their planned remediation. This in turn could result in more disruptions at the transition.

How long might disruptions last? Russia may continue to experience Y2K-related problems in some sectors for months after the New Year. It could take some time for any temporary fixes to be replaced by permanent solutions. It will be prudent to view post-Y2K Russia in a similar way that we are viewing pre-Y2K Russia—as a country that may continue to rely on the U.S. and other countries for help in overcoming computer-related disruptions. We will, of course, maintain a close contact with key Russian sectors after the New Year to continually assess developments.

Depending on the severity of these problems and their effects on ordinary Russians, we will need to come to a decision on the most effective U.S. response. Continued visits by U.S. experts likely will be essential. After the New Year we will have the advantage of knowing where Y2K disruptions have occurred, making us better able to direct our help accordingly.

Cooperating with Russia in these areas, as we've done in the run up to Y2K and as we will continue to do after the New Year, is in the interest of both our countries.

By overcoming the vulnerabilities that come to light during the Y2K transition, Russia may, in the longer term, emerge with a stronger basic infrastructure, enhancing the country's economic potential. Our cooperation in the nuclear energy sector will ensure the continued safe operation of those power plants. Perhaps most importantly, the close collaboration between our militaries to minimize Y2K problems will result in both our countries being less vulnerable to accidental missile launches, in better communication links between the leaders of our countries, and in enhanced security of Russia's nuclear stockpile.

Mr. Chairman, thank you again for the opportunity to address the committee, and for the leadership you and your colleagues have demonstrated in maintaining a focus on this complicated but vital issue. We look forward to keeping in touch with you as we continue to work with Russia to ameliorate the impact of the Y2K problem on American interests.

PREPARED STATEMENT OF RICHARD A. CONN, JR.

Mr. Chairman and members of the Senate Special Committee on the Year 2000 Technology Problem. Thank you for inviting me to discuss potential effect of Y2K disruptions upon business in Russia. My name is Richard Conn. I am a partner at Latham & Watkins, former managing partner of its Moscow office and former head of the foreign bar of Russia. I am here today as Chairman of the Legal Committee of the U.S. Russia Business Council, the leading U.S. based trade organization representing the private sector's interests in Russia. It is a non-profit organization dating back to 1993 with 250 members ranging from entrepreneurs to the most prominent Fortune 500 companies. I would like to thank the American Chamber of Commerce in Russia and the Russia Chamber of Commerce and Industry for their analyses of these important matters. They have graciously allowed me to provide this Committee with many of the findings and suggestions outlined in their recent White Paper, "The Russian Impact of the Year 2000 Problem on Citizens, Businesses and Governments."

In the context of Russia's many problems, Y2K issues appear relatively small. Today, Russia is on the brink of internal unrest as a result of recent bombings in Moscow, its currency remains unstable, its government lacks credibility internally and internationally, and its banking system remains weak. In short, as serious as Y2K issues are, they simply are not perceived as sufficiently serious and immediate to warrant the attention that we in the West feel they deserve.

It is likely that Y2K will cause disruptions in much of the infrastructure of Russia.

- Recent assessments indicate that significant disruptions and negative economic impacts are likely in the short-term though uncertainty exists regarding the extent of the disruptions.
- While awareness has increased, the amount of remediation still required is daunting. The problem continues to be underestimated and full-scale actions to address the problem have only recently begun in some industry sectors and in the government.
- The Russian government faces a major administrative challenge in the face of significant stumbling blocks to promote active remediation economy-wide.
- Russia's unique environment and societal considerations will mitigate the long-term consequences of Y2K disruptions.

The Russian government's response has been weak due to political and economic turmoil. At this late date, remediation efforts should focus on contingency planning. Even if Russia had unlimited funds, all problems could not be corrected in time as the deadline for compliance is fixed. Given its poor financial condition and weak institutional controls, few steps likely will be taken over the next 100 days. Russia's lower dependence on technology for day-to-day operations and a historic strategic working around potentially debilitating crises, however, will reduce the harmful effects of Y2K upon Russia.

I. STATUS

Although authorities in Moscow offer repeated assurances that Y2K will not cause disruptions, recent reports indicate that the Russian infrastructure is at risk for failure. Despite declarations of compliance, the cash-strapped government has offered little evidence of the scope and success of their efforts.

The Gartner Report produced by the Gartner Group, an IT industry analyst organization, forecasts that Russia will experience a severe Y2K problem:

- Utilities will operate at 40 percent of capacity for the first two months of 2000;
- Transportation will be disrupted 80 percent of the time and telecommunications 50 percent of the time for a three-month period;

- Hospitals will deal with nothing but emergencies for at least two months;
- Financial markets will be disrupted for 30 trading days; and
- Banks will be disrupted for 20 business days.

A. Status by Sectors:

1. Power:

RAO UES ("UES"), an electricity production, distribution and transmission monopoly in Russia reports that its system will remain fully operative throughout the start of the New Year. In an April 1999 conference, UES's deputy director noted that the Russian system is operating at excess capacity and that the system could afford to lose some plants or stations and still provide full service. UES also reported to have safety measures to avoid a complete grid malfunction.

As the Gartner Report indicates, however, and as the U.S. State Department and British Foreign & Commonwealth office note, the Russian power grid is likely to suffer widespread and prolonged power outages. For most businesses and individuals in Russia, power failure is the most significant risk of Y2K.

2. Oil & Gas:

Transneft, which is responsible for oil pipelines, and Gazprom, the large gas monopoly, have assured the EU Presidency that there will be no disruptions with the transport of gas and oil to Western Europe. Reported nonetheless exist noting that the Russian natural gas pipeline will be interrupted.[1]

3. Transportation:

Official reports note that the Russian Federal Air Transport Service has tested 9,000 systems. According to the Deputy Director of the Federal Air Transport Service only five percent have reported problems and that 30 percent have developed contingency plans.

As of September 21, 1999, Russia had failed to report to the International Civil Aviation Organization (ICAO) on measures to deal with the Y2K bug. Compliance is accordingly doubtful. The Deputy Director of the Russian Federal Air Transport Service, stated that its agency's experts have checked all computer systems and located the components that could cause problems. Early this month, another spokesman for the Russian Federal Air Transport Service said that the sector had spent more than $100 million dollars to ensure the bug would not affect the sector. Aeroflot also released a statement that "company specialists guarantee that Aeroflot will have no troubles as a result of the arrival of the year 2000." The British Foreign and Commonwealth Office however, reported that two-thirds of Russian airports "are sure to have some Y2K difficulties" and advised citizens to avoid Russian airports.

Russia's extensive and much used railway system is based on an extensive range of small and relatively antiquated computers, which are also vulnerable to Y2K.

4. Communications:

There are more than 2000 local service providers in Russia using a large variety of hardware and software. According to Goskomtelekom, Moscow's phone system has been completely upgraded. Systems testing is scheduled for completion in September. However, the deputy head of Goskomtelekom said at a Russia/World Bank seminar in April, that each of the local operators must have a plan estimating the risk of failure. Disruptions are anticipated, however, in the communications due to the cost and complexity of the system.

The British Foreign and Commonwealth Office published the first part of a global guide to each country's Y2K preparations. The report states that there is a high likelihood of widespread failure in Russian communications. The Gartner Group also reports anticipated failures in this sector.

5. Financial Sector:

Industry sources in Moscow expect most of the Y2K problems with Russia's securities market to occur in the banking and stock transfer sectors. On June 23, 1999, the Russian paper *Sevodnya* reported that there are 133,745 computer systems in Russian economic sectors. Of these, more than 42,000 are at risk of malfunctioning. Major banks have the latest technology and have used the best programming expertise to make themselves compliant, but smaller banks are using extremely dated technology.

The central clearing and accounting system for major banks was installed in 1997. There has been no official statement from the Ministry of the Economy regarding readiness. In July 1999, at a Cabinet hearing, Alexander Ivanov, head of the State

---

[1] See "The Millennium Reckoning," September 1999 Update at *http://www.trendmonitor.com*. Russia Gazprom Natural Gas Pipeline network uses IBM 360 and 370 series computers, which likely contain bugs. Further, monitoring systems were purchased years ago with Y2K problems. Many of the equipment stations containing embedded microprocessors are located in remote locations in Siberia.

Communications Committee reported that the Russian Central Bank was prepared. The main Central Bank branch in Moscow, however, is informing its bank clients that reports show approximately 20 percent of banks may suffer Y2K failures.

Sources also report that Russia's largest exchange, the Russian Trading System, is already compliant. The problem will be in determining whether registrars responsible for maintaining shareholder records, who are far from the main business hubs of Moscow and St. Petersburg, are prepared. Most of the large brokerages appear to be prepared.

6. Status Summary:

In short, developing a picture of Russia's Y2K status requires piecing together often-contradictory pieces of information from numerous sources. We believe that the U.S. State Department's analysis of the current status anticipating disruptions in key sectors of electrical power, heat, telecommunications, transportation, and financial and emergency services is probably the most reliable information available.

II. RUSSIAN GOVERNMENTAL AND PRIVATE RESPONSES

A. Russian Government Response

The Russian governmental performance has been mixed.[2] Its first significant step toward Y2K readiness occurred in May 1998 when former Prime Minister Sergei Kiriyenko demanded that all government systems be made Y2K compliant by the end of the year. No serious effort was made to carry out his order. In January 1999, Russian Prime Minister Yevgeny Primakov set up a government commission ("Commission") to coordinate efforts by central and local government, state, and private institutions to combat the millennium bug. In January 1999, the Russian Government assigned Goskomsvyaz, the Ministry responsible for information systems and communications standards, to be responsible for Y2K.[3] The Commission was also to coordinate efforts by central and local government, state, and private institutions. The order required every Russian state organization to submit quarterly reports to the government commission on it preparedness. However, little reporting has actually occurred. The lack of reporting makes it very difficult to gauge how key infrastructures have progressed and whether reports of compliance are credible. Alexander Ivanov, head of the State Communications Committee reported, for example, that of the 28,000 vital computer systems of government agencies, only one-third are ready for the changeover.

Just months after the Commission was created, it announced a "National Plan of Actions for Solving the Year 2000 Problem in the Russian Federation." The plan outlined nine areas for remediation[4] and attempted to create a national bureaucratic infrastructure, methodologies, and timelines to help organizations develop and implement remediation plans. The response by agencies has been slow. Vladimir Bulgak, acting deputy prime minister, reported that as of May 7, 1999, not a single ministry or department had applied for money to finance remediation. In addition, twenty departments had not even submitted plans on how they would handle the problem.

One of the elements of the plan was the development of "Competency Centers." This was an ambitious plan to have technical consulting centers all over Russia. Establishment of these centers has been relatively successful. As of June 11, 1999, about 162 centers were certified. The centers provide information and consulting for technical and administrative questions. Many private organizations utilized these services and became compliant in March and April of 1999. However, there continues to be a shortage of funds and competent personnel to provide needed technical assistance.

Full implementation of the plan was thwarted, however, as funding was limited, no enforcement mechanisms existed to ensure action, and little accountability was assigned. Benchmarks for compliance and calls for reports were continually postponed or ignored by various agencies.

President Boris Yeltsin added his voice to Y2K compliance by issuing a presidential decree on June 17, 1999, requiring that personal supervision be established for enacting measures for Y2K compliance at all levels of government and "other organizations." In addition to executive action, the Russian State Duma attempted to enact a legislative framework for Y2K remediation by enacting on June 24, 1999 a Year law. The law had provisions which made government agencies responsible to take measures to avoid system failures, established the right of users of tech-

---

[2] For a detailed analysis of Russian governmental action see William McHenry, "The Russian Federation's Y2K Policy: Too Little, Too Late?" *Communications of the Association for Information Systems,* Vol. 2, Art. 10. (August 1999). See, *www.msb.edu/faculty/mchenryw/personal/pubs/cais210.htm*.

[3] In June 1999, Goskomsvyaz was reorganized into Goskomtelekom.

[4] See *www.ptti.gov.ru/gk-doc/2000/natplan.doc*.

nology to demand compliance statements from providers, established rules requiring certifications of compliance from computer system owners, and assigned penalties for noncompliance in accordance with existing laws. President Yeltsin rejected the law, however, in late July 1999 on the grounds that it violated separation of powers.

The failure to establish a legal framework for Y2K has hindered remediation efforts. Such a law could have created mandatory obligations for cooperation and information sharing. There continues to be little direct accountability for government officers to develop and implement economy-wide remeidation plans. This lack of accountability and organization is exacerbated by the frequent changes in governmental leadership.

On a local level, administrations of large cities such as Moscow, St. Petersburg and Novosibirsk have established Y2K related departments to help businesses solve Y2K problems. The upcoming governors' elections and the elections to the Duma in December 1999 have served as an impetus for this activity in the regions. Current political leaders hope to gain credit for their work to solve Y2K problems or at least be able to avoid blame for failures.

Lack of funds is a major impediment to Y2K remediation. The costs of achieving governmental compliance vary widely. Although Russian Finance Minister Mikhail Kasyanov estimates that the government will budget $187 million for Y2K remediation, some experts estimate that Russia needs to exceed that figure tenfold to meet its requirements. Minister Kasyanov's figure was dramatically lower than the previous figure of $1 to $3 billion and no explanation as to the reduction was provided. High-end estimates place the cost of compliance at $12–15 billion, almost half the entire 1999 State Budget. This, of course, assumes that time was available to act.

Due to the lack of funds, the government stated that its focus is upon strategically important branches of the economy, such as defense, transport and energy. In an effort to find more money to address crucial issues, on September 24, 1999, Russian Prime Minister Vladimir Putin signed an authorization to borrow $50 million outside Russia for the Y2K needs in federal organization.[5] In addition, the State Duma passed a bill on September 17, 1999 requested two billion rubles, roughly $80 million dollars, for Y2K problems.

B. Private Responses

Certain sectors of the Russian economy have done very well in Y2K remediation. Financial institutions, large enterprises and multinational organizations are relatively compliant. Larger companies have been able to secure funding, but their remediation efforts may not be entirely complete. For example, in St. Petersburg, the phone company's service is anticipated to work well, but the billing system is not compliant due to lack of resources.

Smaller companies face greater problems because they do not possess the resources to address the problem. Many of these companies are simply planning to have their offices fully staffed at the New Year to manually work around the problem. These small companies receive little assistance from the government since their compliance is not considered critical.

Fortunately, among small businesses, computers are relatively new and cutting edge, or non-existent. The business sector is relatively young (12–15 years), so the level of information technology in the sector as a whole is low. It consists primarily of firms engaged in selling-buying businesses in food products and consumer goods. These small and medium-sized businesses may experience problems in accounting, financial management, sales, client service, information management, and product supply shortages as computers are used in inventory and distribution management systems and for accounting purposes. Some embedded chips may exist, but a private business' primary vulnerability to the Y2K problem is their reliance on utilities. When asked about their own remediation efforts, one U.S. company doing in business in Russia responded, "We have done everything to make our own internal systems compliant. We have received compliance verification from those with whom we do business and from the banking system. However, our greatest vulnerability is the infrastructure of the country. All we can do is hope for the best."

III. FACTORS LEADING TO Y2K INACTION

Russia has exhibited a low level of awareness to Y2K problems. Its ability to respond adequately has been limited by a number of factors.

A. Continued Crisis in Russia

The slow response may be attributed to the fact that Y2K issues are dwarfed by the ongoing crisis in Russia. Almost a decade after reforms began, the economy is

[5] The Federal Ministry of Finance and Vnesheconombank are to negotiate with international lenders. The Ministry of Trade is to control payments and pricing, while Goskomtelekom is to report on the efficiency of the loans' use. Funds from the federal budget will be used to repay the loans.

still ailing. The August 1998 default and simultaneous devaluation devastated the country. The banking system failed and is now just beginning to be reorganized. The cabinet is frequently reshuffled. Roughly 60 million people, almost half the population, live below the poverty line. Income inequality has risen; life expectancy has plummeted. Violence in Moscow related to regional conflicts threatens to reopen conflicts in Russia's southern provinces. In the context of these issues, Y2K problems do not garner serious attention.

B. Lack of Awareness and Appreciation of the Problem

As recently as 1998, there was considerable skepticism in Russia as to the risks imposed by Y2K. Vladimir Bulgak, head of the Commission for the Y2K problem was of the opinion that those who wished to market technical equipment and services exaggerated the threat. A Nuclear Ministry spokesman said in June 1999 that his agency would "deal with the problem when we get to 2000."

C. Lack of Funds

Many Russian companies are already months behind in payroll and taxes, lack working capital or have had funds frozen in Russian banks. The public sector fares no better with severe budgetary constraints. As time continues to run out, the costs of making systems compliant rise proportionately and exacerbate the funding problems.

D. Lack of Experienced Y2K Professionals

Since Russian companies have not had adequate capital to address these problems, many companies have reduced their IT staff, causing former employees with technical skills to leave the country for more financially rewarding opportunities. These skills have been in demand in the West for years. Other companies have transferred their staff to assist in operations abroad. The net result is that Russia has lost a significant amount of personnel to work on the problem.

E. Antiquated Computer Systems

Vivek Wadhwa, the CEO of Relativity Technologies, a North Carolina company that sold the Russian government the software to fix its Y2K problems explains the situation: "There are, I think, about 4000 mainframes in Russia. All of those mainframes have a year 2000 problem, without exception. The Y2K problem, from a technical point of view, is probably more intense in Russia than it is here, because in addition to having the American hardware and American computer languages, they also have Russian hardware, and languages that are not used in the West anymore."

F. Lack of Cooperation

Distrust is pervasive in Russia. Russia initially resisted the idea of international cooperation. When the U.S. approached the Russian about sharing early warning data to help prepare the Russians for Y2K, a faction in the Russian military believed it was simply an attempt by the U.S. to infiltrate Russian security.

Fear and misunderstanding has led to little trading of information. For instance, one bank with Y2K bugs refused to let consultants look at its computer code, calling it a trade secret. This distrust and lack of cooperation has frustrated remediation efforts as each institution is required to assess the problem itself and attempt to solve it with limited resources.

G. Difficulties in Identifying Non-Compliant Systems

In the West, manufacturers of technology often will contact customers if systems are non-compliant or otherwise make information available. Organizations often cannot rely on manufacturers to inform them of noncompliance in Russia. Much high-tech equipment was either imported by middlemen who are no longer in business, imported through third countries in order to avoid export controls, or purchased by centralized government buying agencies who did not reveal the end destination of the equipment. Users of technology, therefore, either struggle to identify the producer of a system or attempt to determine compliance without the manufacturer's assistance.

Similar problems exist for domestic equipment produced by government or former government factories and institutes. Many factories are no longer in existence. In the past, secrecy prevented some companies from maintaining accurate records. To further complicate the issue, many employees who designed the system have left the area or even the country.

Whether associated with foreign or domestic systems, piracy also makes assessment of Y2K problems difficult. Many companies use a pirated version of software. Accordingly, the manufacturer cannot or will not contact the company to recommend upgrades for compliance, since the company with pirated software is not a registered owner.

The net result of these factors is that it is difficult to identify the components and manufacturers of different systems. Even if an organization is able to locate a manufacturer, poor telecommunications and a language barrier discourage contact.

IV. RUSSIA'S MITIGATING CIRCUMSTANCES

The potential Y2K failures outlined above would be disastrous for the United States, but the history and present economic situation of Russia suggest that Y2K will not have as catastrophic an impact on Russia. First, technology is not as pervasive; there are fewer system to fix. Russia has far fewer digital control systems and computers used in industry and government than in the West. While the West has computerized most systems, most in Russia are analog and electromechanical. For example, most elevators, heating and ventilation systems, and shop floor equipment in Russia are electromechanical. Further, in the West, most desks in an organization are centered on a personal computer with business processes conducted via software. In Russia, it is not standard to have a computer at a work desk. During Soviet times, personal computers were strictly limited. And indeed in many areas of Russia, it is a rarity. For instance, clerks in many Russian shops continue to use an abacus. In addition, few government services are computerized. Functions such as welfare rolls and the military draft are still carried out manually on paper.

The second advantage for Russia organizations is that they are well versed in working around the type of disruptions that Y2K will create. In the West, most companies have built their organization around stability and predictability. Most Western factories have precise supply chains and do not keep large inventories. For instance, recently when one important supplier of General Motors went on strike it bought production to a standstill. In Russia, businesses operate with unreliable supplies of everything from power, water and other raw materials to transportation. Many, if not all, Russian companies, and especially smaller companies, have experienced loss of contact with distributors and retails, supply chain breakdowns, disruptions in transportation and utility services, or frozen accounts for years. Most Russian managers have developed the expertise to quickly adjust and work around problems.

In addition, most individual Russians are familiar with interruptions in power, telecommunications, transportation and other major utilities. There is reason to believe they will not experience the anxiety and potential overreaction that threatens Western nations.

A final factor cushioning Y2K's effects in Russia is that some computer systems that have been purchased by businesses are relatively new. Many were either purchased Y2K compliant or are easily converted to compliance.

V. RECOMMENDATIONS FOR ACTION

A. The Russian government should identify systems of national and international importance and ensure there are "triage" plans for them. A Ministry, e.g., the Ministry of Emergency Situations, should be assigned the responsibility to coordinate the plans that are developed. These may include but are not limited to:

- Communications—telecommunications and data networks, Rostelekom and Svyazinvest
- Emergency Services—police, ambulance and fire, Ministry of Emergency Situations
- Energy—generation and supply, Gazprom, RAO–UES, Transeft
- Finance—banking and trading, Central Bank, Sberbank
- Food Supply—shipping, storage and distribution
- Manufacturing—supply chains and automated process control systems
- National Security—defense and intelligence services, Ministry of Defense
- Public Health—hospital equipment and systems, medications and supplies
- Finance Ministry—tax collection, customs and excise, and pension payments
- Transport—air and rail traffic control systems, mass transit systems, navigation systems
- Utilities—water supply and waste management

B. Each Ministry and organ should immediately allocate sufficient financial and human resources to fix the most essential Year 2000 problems for its own systems, and take appropriate actions to incentivize regional (oblast, krai, autonomous regions) and local governments to do the same.

C. The Russian Government should take appropriate action to make the state enterprise sector aware of the need to assess a high priority to the Year 2000 computer problem.

D. Progress should be publicly reported at regular intervals.

E. In addition to the suggestions above, we would encourage cooperation between the Russian and U.S. Governments and coordinating agencies with the following recommendations:

- Ensure active involvement by the Ministry of Emergency Situations and its Minister Sergei Shoygu and coordination with his counterpart at the United States Federal Emergency Management Agency (FEMA)

- Encourage greater involvement in Y2K between the Russian Deputy Prime Minister Bulgak and the American Y2K Director Koskinin.
- Develop a map/diagram of all key infrastructures in both Russia and the United States and show how they interact and interface with each other. Utilize the information for high-level scenario planning.
- Develop an economic scenario for the loss of revenues from exports and imports and determine the potential economic impact on both the Russian and American economies.
- Set up a meeting for all First Deputies of all the Ministries to review scenario planning, contingency planning and business continuity planning for Y2K in Russia with which corresponding departments in the United States can assist.

VI. CONCLUSION

Russia's limited commitment to Y2K will result in a significant economic cost to Russia. The cost of fixing problems as systems fail, in terms of direct costs and damage to the Russian economy, will be much higher than the cost of fixing problems prior to the deadline. In addition, "work around" solutions will prove inefficient by prolonging the life of obsolete systems. In the short-run, the "work arounds" will provide continuity. In the long run, Russia's journey towards a healthy economy will be all the more arduous due to Y2K non-compliance.

PREPARED STATEMENT OF VICE CHAIRMAN CHRISTOPHER J. DODD

Today is the first country specific hearing of the Special Committee. With 94 days to go—actually only about 66 working days and 13 weekends—we want to understand the potential impacts and future consequences Y2K may have on Russian stability. The purpose of this hearing is not to "beat up" on Russia or embarrass them. On the contrary, the goal of this hearing is to understand how Y2K failures, short-term and long-term, may impact current U.S. policy initiatives and what we can do to address these potential problems.

Home to almost 150 million people, Russia spans 12 time zones. Russia is the 30th largest U.S. trading partner and hosts 11,000 U.S. citizens. While it is neither the largest trading partner nor the biggest host of U.S. citizens, we all recognize that Russia has continued to be an important U.S. foreign policy concern for more than fifty years. Since the end of the Cold War, U.S. foreign policy goals with Russia have broadly fallen into two categories: reducing the threat of nuclear weapons and supporting Russia's efforts to transform its political and economic system. Both are long-term goals that, admittedly, will take years to achieve. Russians struggle with many difficult issues including the 80% devaluation of the ruble in August of 1998. In addition, government and financial instability has spurred capital flight of nearly one billion dollars each month. In the past year Russia has lost $15 billion dollars in capital to foreign banks. Now, the country must confront the Y2K challenge.

In March, the Department of State testified that the U.S. would need a "robust policy framework" in order to prioritize responses to international Y2K failures. I am interested to learn what this policy framework will be with respect Russia. Many policy experts have viewed "Y2K" as a short-term problem, one best left to "techies," and not likely to impact enduring policy concerns. Unfortunately, according to Gartner Group, many Y2K problems will only emerge in the weeks and months beyond January 1, 2000. Today, the Committee seeks to better understand Russia's highly unique situation and whether Y2K could erode stability that we take for granted in our ongoing bilateral initiatives.

Before I go any further, I want to specify what I mean by long-term Y2K concerns. Many organizations responsible for key Russian infrastructures lack the money available to make the necessary fixes. For example, Rostelecom, Russia's long distance and international carrier, is reportedly unable to upgrade its 7 gateway switches and is choosing to implement "work arounds." Meanwhile, regional carriers have only just begun testing their networks. Lack of funding will force many to create their own ad-hoc fixes. While these "work arounds" are likely to prevent immediate failures and keep connectivity, they could degrade capacity—in short, Russia could lose communications capacity, stability and profitability. In fact, we will hear testimony today about the fact that six out of the seven direct communication links from Moscow to Washington that are used in times of crisis would experience Y2K failures. Let me emphasize that six out of seven key national security links could fail—and will fail if the fixes are not implemented. These critical links will be fixed, but what about the bulk of commercial communications? The U.S. has to carefully consider the impact of Russian infrastructure failures in our relations with Russia.

Today, we will consider the concerns of the Department of Defense, State and Energy. On September 13, DOD and the Russian Ministry of Defense (MOD) signed an agreement indicating their intent to establish the Center for Year 2000 Strategic Stability during the Year 2000 transition period. In this center, U.S. and Russian military personnel will sit side-by-side and continuously monitor U.S.-provided missile and space launches information. I would like to remind you that Russia still has approximately 6,000 strategic nuclear weapons and over 1,000 delivery systems. The Center will also provide an important link to communicate other defense-related events that could be potentially destabilizing, such as an aircraft going off course due to a navigation or communication system Y2K failure. Last week nine military officials from Russia were in Colorado to discuss the details.

Also last week, the Congress the Defense Authorization bill and it is now waiting to be signed into law. This bill provides over to $475 million dollars Cooperative Threat Reduction. In August, the Ministry of Defense requested $15 million dollars to address Y2K related security risks for the control and protection of weapons grade nuclear materials. As a requirement, Russia must be recertified by the Administration October 1 before any funding can continue. Unfortunately, this recertification process can often take several months. We cannot afford to lose any time in this matter.

Reliable energy is of key importance to the entire nation. In August, the Unified Energy System (UES), the Russian electric monopoly, cut power to some 20,000 customers just to save fuel for the winter. What this means is that fuel reserves for Russia's electric power monopoly will be as low as the country heads into Y2K. DOE is working closely with Russia as it develops the necessary contingency plans that will be needed to maintain grid stability.

Nuclear power plants are a serious concern for Russia. Russia has 29 nuclear power reactor units in operation at nine different sites. Western-style nuclear power plants employ an uncompromising set of in-depth safety elements including a massive reinforced concrete structure, called the containment, to prevent the release of radioactivity. Most Soviet-designed reactors do not have such a containment structure. The most infamous plant without a containment structure is the Chernobyl-style reactor, and there are 11 of these reactors at three locations in Russia. While these plants do not have direct Y2K vulnerabilities, they can only withstand a loss of power for approximately 90–120 minutes before they begin to have core damage. In a country where disruptions in power supply are common before Y2K, special consideration needs to be paid to the months and years beyond Y2K to reduce the chances that sudden loss of power could compromise power plant safety.

Primary plant safety systems are the front line of defense against accidents and no Y2K issues have been found here. However, other systems important to safety and plant operations are of concern such as the plant process computer and information display system. A Y2K-related malfunction in these systems would complicate operations and increase the chances of operator error. Operator error ultimately led to the Chernobyl accident. The combination of human and computer error is one of the greatest Y2K challenges for Russia and the rest of the world.

I would like to thank Senator Lugar for testifying. He has been a tremendous asset to the Y2K Committee. His work on Cooperative Threat Reduction has been an invaluable contribution to nuclear non-proliferation and a legacy that U.S. can be very proud of.

PREPARED STATEMENT OF SENATOR RICHARD G. LUGAR

Mr. Chairman, Senator Dodd, members of the Committee, it is a pleasure to be here today. I appreciate the opportunity to testify on U.S.-Russian cooperative activities in response to the Y2K computer problem.

Since the end of the Cold War, I have taken a great deal of interest in U.S. policy toward the former Soviet Union. As the Soviet Union began to break apart in 1991, Russian leaders came to former Senator Nunn of Georgia and me and pointed out the dangers of the dissolution of a nuclear superpower. The viability of the entire Soviet weapons custodial system was in doubt. There were tons of weapons and materials of mass destruction spread across hundreds of sites in Russia and other former Soviet states. Russia requested our cooperation in securing and dismantling its nuclear arsenal and weapons-usable materials. This was the genesis of the Nunn-Lugar Cooperative Threat Reduction Program.

This was not a problem that Congress wanted to deal with in 1991. The atmosphere was decidedly against any initiative that focused on a foreign problem. Americans were tired from the Cold War and the Gulf War. Yet we brought together a nucleus of Senators who saw the problem as we did. Remarkably, the Nunn-Lugar

program was passed in the Senate by a vote of 86 to 8. It went on to gain approval in the House and was signed into law by President Bush.

While much more remains to be done, the Nunn-Lugar Scorecard is impressive. Nunn-Lugar has facilitated the destruction of 365 ballistic missiles, 343 ballistic missile launchers, 49 bombers, 136 submarine missile launchers, and 30 submarine launched ballistic missiles. It also has sealed 191 nuclear test tunnels. Most notably, **4,838 warheads that were on strategic systems aimed at the United States have been deactivated.** All at a cost of less than one-third of one percent of the Department of Defense's annual budget. Without Nunn-Lugar, Ukraine, Kazakstan, and Belarus would still have thousands of nuclear weapons. Instead, all three countries are nuclear weapons-free.

I offer this as a useful example to cope with another problem that has arisen in our post-Cold War relationship—namely, the impact of Y2K. The atmosphere surrounding the current Russian-American relationship and its implications for our national security are not unlike those that existed in 1991. I believe it is in U.S. national security interests to, again, cooperate with the former Soviet Union to reduce the threats our country may face.

Mr. Chairman, we do not know what is going to happen to Russian computer systems when we pass into the millennium and neither do they; but, initial estimates do not appear promising. In March, the American Chamber of Commerce in Russia pointed to a study that paints a disturbing picture of the impact of Y2K in Russia. "Utilities will operate at 40% of capacity for the first two months of 2000; transportation will be disrupted 80% of the time, and telecommunications 50% of the time for a three-month period; hospitals will be forced to treat only emergencies for at least two months; financial markets will be disrupted for 30 trading days; and banks will be disrupted for 20 business days." Obviously these estimates are disturbing and beg the question of whether similar problems will affect the Russian military and strategic forces.

I am not here to push the panic button. In my visits to Russia and in briefings and conversations with experts on these subjects, I have been convinced that the chances of an accidental missile launch as a result of a Y2K problem are almost non-existent. But Y2K may cause other problems in Russian strategic systems.

It is in our interests to take out a kind of "insurance policy" to ensure that the transition to the new millennium does not exacerbate this situation. Cooperative activities and programs that reduce these threats are in the national security interests of the United States and Russia—provided they are implemented in a responsible manner.

Experts agree that cooperation over the transition period needs to center on three specific areas: early warning systems, nuclear weapon security, and nuclear power plants.

EARLY WARNING:

Our Department of Defense began discussing the potential impact of Y2K with Russian counterparts in June 1998. These efforts culminated in an agreement to establish a Center for Y2K Strategic Stability in Colorado Springs, Colorado. The center will ensure that, for the last few weeks in December 1999 and the first weeks of January 2000, a U.S. and Russian military officers will sit side by side and monitor early-warning data generated by satellites observing missile activity around the world in order to ensure that potential mishaps caused by Y2K do not lead to strategic miscalculations and mistakes.

Mr. Chairman, it is in the interests of the U.S. to ensure that Russia understands the kinds of problems they may encounter with its strategic systems so that there are no surprises or confusion on January 1. We want them to understand that their problems are Y2K-related and not a result of U.S. hostile action or which they need to respond. This requires consultation, awareness of potential Y2K failures, and training of key personnel. This kind of cooperation is clearly of as much value to the U.S. as it is to the Russians.

Russian early warning operators may not be able to tell the difference between a peaceful rocket and a military rocket from their computer screens. *Russian early-warning capabilities continue to deteriorate, and this deterioration will be compounded by the transition to the year 2000.* Russian Major General Dvorkin recently suggested that Y2K problems could lead to incorrect information being transmitted, received, displayed, or complete early-warning system failures. We should heed these concerns. I am sure we remember the convulsions the Russian command and control system endured several years ago when a peaceful Norwegian rocket launch activated President Yeltsin's nuclear briefcase. Fortunately, the Russians realized their mistake.

The Center in Colorado is meant to create an atmosphere for both sides to work together to resolve any missile launch detection, false alarms, or other ambiguities

that may arise. I am hopeful that the Russian military officers serving on the second floor of building 1840 at Peterson Air Force Base will, in the event of a Russian malfunction, be able to provide Moscow with the accurate information and data necessary to eliminate misperceptions.

NUCLEAR STOCKPILE SECURITY:

The continuous safe and secure storage of the Russian nuclear stockpile is the second area that will be complicated by Y2K. Over the last six or seven months, the Department of Defense has sought to engage its Russian counterparts on the nuclear warhead protection, control and accounting systems. Early in the discussions, the Russian Ministry of Defense admitted that it had not considered the impact Y2K could have on their systems. The need for U.S. assistance in this area is clear. As members of the Senate, we all have had countless briefings on the groups and individuals attempting to illicitly acquire these weapons.

More recently the Russians have made substantial progress in acknowledging and responding to these potential problems. The Russian Ministry of Defense has committed to establishing and maintaining special Y2K monitoring stations at their largest nuclear warhead storage facilities. Stations will be manned 24 hours a day by officers specially trained to monitor physical security, environmental controls within the facility, telecommunications, and power levels. These efforts and accomplishments mark a tremendous improvement.

At Pentagon urging, the Russians have conducted capability assessments to gauge their ability to respond to an emergency. Unfortunately, the results of the assessments were not encouraging. Due to the lack of appropriate response equipment, it is clear that there are significant deficiencies in their capabilities to respond to intrusions and other potential threats. Our Defense Department is seeking to assist Russia in these efforts through the Nunn-Lugar program.

The Russian Ministry of Defense has requested approximately $15 million in equipment to upgrade their ability to respond to an emergency. I understand that Assistant Secretary of Defense Warner will testify later, so I will not attempt to describe the details of the assistance. But I have been told that the Pentagon has reviewed the request and has determined it to be reasonable and consistent with Nunn-Lugar conditions and restrictions.

Mr. Chairman, the Pentagon reports that a portion of the request can be fulfilled immediately, using prior year Nunn-Lugar monies. However, the remainder of the Y2K assistance must await a re-certification requirement in the FY 2000 Defense Authorization Conference Report. The Executive Branch is hopeful that the process will be completed on or around October 1. But Mr. Chairman, this committee must watch this situation closely. I believe the delivery of this assistance to be in U.S. interests. Delays in the re-certification process might possibly slow Y2K assistance to the point where the equipment arrives after the first of the new year. The Senate must view this additional and redundant re-certification as a self-inflicted wound that must not be permitted to interfere with important national security goals. This committee, the Senate Armed Services Committee, and the Committee on Appropriations must be prepared to expunge such a duplicative requirement should American interests dictate.

NUCLEAR POWER PLANTS:

The potential threats emanating from Y2K problems in Soviet-designed nuclear reactors is a third area of concern. Historically, safety mechanisms and procedures at these reactors are poor. The reactors suffer from deficiencies in design, operator training, and safety procedures. Reactor operators and support staff face low and erratic pay, training shortfalls, and deficiencies in safety procedures. Unfortunately, these problems are compounded by a very late start in preparing for the transition to the new millennium by the states of the former Soviet Union and Central and Eastern Europe. Although neither a melt-down or a failure of primary safety systems is likely, it is in our interests to continue to work to prevent these potential threats.

Many believe that Soviet-designed reactors are immune to Y2K-generated problems because they utilize older analog systems. This is incorrect. Digital overlays were installed to improve performance, monitoring, and safety response and are susceptible to Y2K problems. If these systems were to malfunction, operators could be blind to some reactor functions or receive erroneous data that could lead to improper actions. In U.S. reactors, this would not pose a problem because of built-in redundancy of our systems. Unfortunately, redundancy is not present in most Soviet-designed plants.

Reviews of Soviet-designed reactor susceptibility to Y2K-induced problems revealed that host countries lacked the resources to conduct threat evaluations and significant safety issues were at stake. Officials of the Department of Energy

worked closely with their counterparts to develop assessment guidelines in order to determine potential problems that might arise during the millennium transition.

U.S. expert assistance was crucial in overturning initial complacency expressed by these nations. The Department of Energy played an important role in completing the detailed risk assessments of the various Soviet-designed reactors and providing assistance to begin remediation of hardware and software problems. It is clear that without the Department of Energy's efforts, the risks of an accident would have been much higher.

Given the existing time frame, it is too late to fix every Russian system. Our efforts must continue to concentrate on reactor safety systems, contingency planning, and engagement with the Russian Ministry of Atomic Energy on these subjects. Transparency and consultation in these areas are in U.S. interests. Furthermore, I believe our country must make every effort to warn Americans abroad, living or working near these reactors, of the problems they may face as a result of Y2K.

One of my personal concerns is the impact of local and federal government pressure to keep Soviet-designed reactors on line in the face of strain and uncertainty. It will be the dead of winter with temperatures dropping far below freezing. Local and state governors and mayors, as well as officials in national capitals, will be loathe to permit nuclear reactors to shut down. Political pressure, in addition to monitoring failures and a loss of off-site power, may contribute to failures in judgment, which could lead to accidents.

Recently, Russian Atomic Energy Minister Adamov reported to a conference in London that he believed that Russia had achieved "the same level of safety as Western units". He went to explain that the rate of unplanned shutdowns at Russian reactors was equal to that of Germany and lower than France and the United States. I am hopeful that his confidence is borne out, but it is in our interest to continue to cooperate in alleviating the problems inherent in the 65 nuclear reactors at 20 sites in 9 countries of the former Warsaw Pact and former Soviet Union. If not handled properly, these reactors could prove threatening to American interests. We must not forget that one of these sites is less than 130 miles from Alaska.

CONCLUSION:

Mr. Chairman, I began my testimony with the recommendation that we view efforts to eliminate potential threats to U.S. security from Y2K generated problems in Russia as an "insurance policy." In my opinion, an insurance policy in this area is a good investment. The cost of efforts to address potential threats today will be minuscule in comparison to the costs of responding to a tragedy should an accident occur.

Mr. Chairman, I understand that the atmosphere today may not be all that conducive to engagement and cooperation with Russia. Congressional committees are investigating allegations of corruption by Russian government officials. As I indicated in my introduction, the Senate has faced similar circumstances before. There are many parallels between the mood today and that which Senator Nunn and I faced in 1991. I would urge my colleagues to once again look to the future and to examine the benefits of cooperating with Russia on Y2K versus the potential costs of inaction.

In 1991, the Senate courageously supported the Nunn-Lugar program in the face of widespread discontent with foreign affairs. That investment has paid tremendous dividends to our national security. I would urge this Committee and this Congress to once again provide our country with the leadership necessary to protect our national security. I am not suggesting that we send Moscow a blank check. But our government must again engage the Russian people through the auspices of the Departments of Defense and Energy and our private sector. Strict management and accountability of cooperative efforts with Russia will protect our investments as it has through the Nunn-Lugar program. We have made important progress, but it is clear that there is still much work to be done.

Mr. Chairman, Senator Dodd, members of the committee, I praise your foresight in examining these issues, and I look forward to working with you to address the threats facing our country.

Thank you.

PREPARED STATEMENT OF DR. WILLIAM K. MCHENRY

I. INTRODUCTION

Chairman Bennett, Vice-Chairman Dodd, and Members of the Committee, thank you for inviting me to testify. I would like to commend you for the leading role you and others have played in promoting Y2K readiness here in the United States and in helping U.S. business and government to prepare for possible effects of the Y2K

problem from other countries. I am an Associate Professor at the McDonough School of Business, Georgetown University, where I am also affiliated with the Center for Eurasian, Russian, and East European Studies in the School of Foreign Service. For the past 20 years, I have studied issues of information technology and its diffusion in the economies of the Soviet Union and Russia,[1] and have participated in a number of U.S. government-led panels and studies regarding issues of technology transfer.[2] Most recently I performed a study on the Russian Y2K problem for the Mitre Corporation, and wrote a paper for the *Communications of the Association for Information Systems* with Leonid Malkov, upon which this testimony is partially based.[3]

The Y2K problem in Russia is taking place against a backdrop of extraordinary economic problems and considerable political uncertainty. Indeed, Yabloko politician Gregory Yavlinsky was heard to remark that Russia's real Y2K problem is Boris Yeltsin. What impact can potential computer failures have when GDP has declined an estimated 43 percent since 1991?[4] Or when the Russian Unified Electrical System says that it only has 60 percent of the fuel oil it needs for the fall-winter season?[5]

II. OVERALL ASSESSMENT

In some respects the situation in Russia is no different than the situation in many other countries. There will be some systems that fail as a result of the Y2K problem, but it is difficult to say precisely which ones, or exactly how great an impact this will have. As you will see from some of the data presented here, the Russian government has frequently changed its assessments of the cost of remediation and the number of systems affected. I liken the impact to a number of blows during a boxing match: many other blows are coming from other sources, and it is difficult to say just which blow may lead to a knockdown.

There are two main reasons for this state of affairs in Russia: first, remediation efforts started rather late, and second, financing remediation work and purchases of new hardware and software have been extremely difficult.

The Late Start

The first serious efforts for remediation in Russia came only after a decree by then Prime Minister Kirienko in May, 1998. By December, 1998, there had been hearings in the Duma and a strategy for addressing the problem had been initiated. Practically from the start, Vladimir Bulgak, who was then Deputy Premier and the highest ranking official tasked with the Y2K problem, stated that not all systems would be able to be remediated in time. In mid–1998, the government reported that it had 96,000 computer systems, of which 51,000 were potentially subject to the Y2K problem.[6] Novell reported that as many as 90 percent of all local area networks in the country used Netware,[7] and that there were 300- to 500,000 workers in the Russian government structures using mostly earlier, non-compliant versions.[8]

In May 1999 the government reported that there were 50,681 computer systems in its ministries and departments, of which 16,040 (31.6 percent) were critical. It was planned to fix 17,747 at a cost of $657 million, leaving 65 percent of all 50 thousand systems un-remediated.[9] By July the estimated total number of systems had been increased to 152,200, of which 30,300 (19.9 percent) were considered critical.[10]

The May 1999 data present the most detailed, comprehensive view of the situation in a number of sectors, and shows the wide disparities in what are considered "systems" and the potential magnitude of fixing them (Appendix One). For example, the security-related ministries, including the FSB and the Ministry of Internal Affairs, reported only 48 critical systems. The repair cost per system, however, was $1.3 million versus an average cost of $58,000 for all the other ministries and departments, indicating that remediation of these systems would be significantly more complicated.

One of the cornerstones of the government's approach to solving the Y2K problem was to designate state, private, and academic organizations as "Centers of Competency." The centers represented a good idea of leveraging the relatively small amount of available expertise and giving all organizations visible places to get help. Rather than provide government-financed services to needy organizations, however, these centers have required payment, which has reduced the number of clients dramatically. Some are leading systems integrators, while others are organizations that are descended from (perhaps even the remnants of) Soviet institutes. In some quarters their reputation is poor. Furthermore, by June 1999 they were present in only 51 percent of the administrative regions of Russia. Only nine regions, including Moscow, had more than three centers.[11]

Throughout the first months of 1999 there was the expectation that Boris Yeltsin would sign a Y2K Problem decree. He finally did, but only in June. The development of a National Plan for Y2K Remediation was financed by The World Bank, but was published only in March. Legislation was expected that would clarify who was responsible for Y2K problems, resolve the question of finances, and mandate remedi-

ation of critical systems. Such a law was finally passed, but Yeltsin rejected it.[12] Cooperation with the US Government on the joint monitoring of early warning data was delayed by the Kosovo conflict.

Financing

Financing has been a key problem. No ministries and departments made specific line-item requests for Y2K financing for the 1999 budget, and Parliament did not allocate any funding for it. Throughout most of 1999, most government agencies were told that they had to reallocate funds from within their existing budgets for remediation work.

Making sense of the statistics offered by the Russian government and other sources about costs of remediation has been difficult. At first the estimate was $500 million, then it became $2–3 billion in the early months of 1999. Adding up published estimates by individual ministries and departments yielded a total close to $1 billion. Fixing the 17,747 systems as of May 1999 mentioned above was estimated to cost $657 million.[13] In June 1999, the estimate was back to around $471 million.[14] In mid-July the government said that 2 billion rubles ($80 million) had already been spent, while another 11 billion rubles ($458 million) would be needed, or a total of $538 million.[15] On September 24, 1999 the Duma approved a bill for a supplemental appropriation of up to 2 billion rubles ($80 million) for Y2K remediation which is now being sent to the Federation Council and then will await President Yeltsin's signature.[16]

On September 23rd it was reported that Prime Minister Putin has signed an order authorizing Goskomtelekom to seek a $50 million credit to buy hardware and software in the West.[17] As you know, a great deal of time is needed to check, repair, test, and re-introduce complex information systems. With the expected delivery of new hardware in October or November, it is quite difficult to believe that systems based on this equipment and software will be fully ready by January 1, 2000.

And so, as a whole, the Russian government planned to skip fixing a large number of systems before January 1, 2000. At the end of July it was still estimated that only 30–35 percent of systems had been remediated. To my knowledge no new overall assessment has yet been published. These data also do not reflect the status of regional governments and private industry. All indications are that "the regions" for the most part have lagged behind the central government. Very limited data has been available about the extent to which private firms have taken up the Y2K problem.

Nevertheless, representatives of important infrastructure components such as energy, banking, and telecommunications continue to assert that the necessary remediation will take place in time. The large amount of work which is now going on is reflected in the fact that Novell has seen a very significant rise in business from government institutions and industrial enterprises, particularly in the second and third quarter of 1999. One of the top managers in the Moscow office believes that 90–95 percent of their customers will be ready.[18]

III. THREE KEY INFRASTRUCTURE SECTORS

I have been asked to address the Y2K status of the energy, the banking, and the telecommunications sectors. Sources of information for these assessments rely heavily on self-reported data. If I were to report close to 100 percent remediation, there would be reason to question the veracity of the data given the late start. However, most of the data seems to be fairly realistic, even in the way it changes from month to month.

The Energy Sector

In the electrical power generating sector, the biggest concern has been and continues to be the operation of nuclear power plants. I have written more extensively about this elsewhere.[19] My overall assessment is that nuclear accidents due to the Y2K problem alone are quite unlikely. The potential that some systems within nuclear plants will have problems cannot be ruled out, especially since some indigenous Soviet technology remains in use. But the plants have been the subject of a great deal of attention and some funding from a number of Western sources, and remediation work seems well underway.[20]

The Unified Energy System (EES) is clearly taking the Y2K problem very seriously, and has defined teams at all levels of its hierarchy to address the problem. As of May 15, 1999, the energy sector had received information about telecommunications equipment deployed in the sector from 70 percent of the foreign and domestic vendors.[21] According to a June 1999 briefing, the energy system had 50,000 computers just in the more critical control functions, of which 17,000 needed to be replaced at a maximum cost of $45 million for the whole sector.[22]

The EES released extensive data at a presentation in July, 1999 (Appendix Three). The branch as a whole had about 2,500 computer systems, 66 percent of which were considered critical. About 35 percent had been modernized or put into

service. Required financing was about $30 million, of which about 20 percent had already been spent (and 80 percent remained to be found). Financing from the budget of the Unified Energy System was provided for the Central Control system, seven regional control systems, and the main computer center. It was recommended to other energy firms and electrical stations to seek permission to raise tariffs to cover Y2K costs, which was granted in some cases.[23] It was expected that the whole system would be brought into compliance by October, 1999.[24]

The Fuel-Energy complex reported in mid-July that it needed $96 million for remediation, including $66 million for hardware and $29 million for software. Only 1/3 of those funds were expected to come from the central government.[25] According to the May 1999 inventory (Appendix One), 26 percent of 8,215 systems were critical, and 34 percent of these had been renovated or put into operation at that time.

In the oil industry, some companies have published quite a bit of information about their situation while others have published little. LUKoil, the largest oil company, issued an April 1999 press release in which it claimed that only 7 percent of critical systems were not ready for the Year 2000. It is among a small number of Russian firms installing SAP's R/3.[26]

Yukos, the second largest oil company behind LUKoil, described its Y2K remediation efforts in February 1999. It expected to spend $8 million. Yukos planned to carry out research, create an inventory, and so forth, from Dec. 1998 to March 1999. A planning stage, which encompassed a plan for replacement, presenting a budget for the project, and planning what to do if there is a crisis situation, was to be done in February-March 1999. In March-November 1999, Yukos intended to realize the plan for replacement, including replacing "a rather large stock" of Soviet-era mainframes (Lukoil said that it had already eliminated 1980's technology). The final stage of work, handing over the work and general verification of safety, is not planned until Dec. 1, 1999.[27] It is hard to believe that Yukos will be able to order new mainframes, install them, and convert everything with adequate testing before Jan. 1, 2000.

Yuganskneftegaz, another oil and gas concern, posted a preliminary analysis of its situation to the Web, noting that they had not had centralized control over hardware and software purchases, which alone led to the use of around two dozen different accounting packages from many different vendors.[28]

Gazprom reportedly started work in 1997, and by February 1999 was reporting that all remediation work had been completed in computer networks; drilling, extraction, and delivery of gas; and gas transport systems.[29] However, a May 1999 inventory of just the telecommunications equipment at Gazprom found 1,450 pieces of communications equipment subject to the Y2K problem. The remediation cost was estimated to be $15.7 million.[30] According to a Gazprom presentation in July, 1999, the inventory and testing stages had been completed for all its systems. Only 14 percent of systems, including process control and telecommunications systems, were critical for the Y2K problem. Most of the control systems used older technologies from the 1970's and 1980's. As of June 10, 1999, more than 58 percent of all critical systems had been modernized, with all the rest planned to be finished by October 1, 1999.[31] In August 1999 Gazprom stated that somewhat less than half of these systems had yet to be remediated.[32] In the fourth quarter acceptance of the modified systems is to be completed, and most attention is to be paid to working out actions based on the contingency plans.[33]

If any sectors have funds available for Y2K remediation, it is the hard-currency producing energy firms. In addition, these sectors are receiving obvious and extended scrutiny. There are limits to the effectiveness of this administrative approach, but in this area, where the stakes are very high, I believe sufficient attention will be paid to ensure that severe effects will be avoided.

The Banking Sector

During the 1990's the Russian banking sector was one of the leading purchasers and users of hardware and software in Russia. Many of the best programmers were recruited, and a number of banks wrote their own banking software. Other banks bought turnkey packages and modified them.

It appears that this sector was one of the first to become concerned about the Y2K problem. Nikolay Egorov, Deputy Head of the Central Bank of Russia, gave an interview at the end of 1997 to *Computerworld Russia*, which is one of the earliest statements about the Y2K problem by any governmental official that we have been able to find.[34] As of September, 1998, there were 1,500 banks in Russia, according the Central Bank head Viktor Geraschenko. The fact that he expected no more than 200–300 to survive illustrates the disjunction between the magnitude of the Y2K problem, on the one hand, and the overarching economic problems in Russia, on the other.[35] The Central Bank of Russia issued an Order in September 1998 which out-

lined four stages of Y2K remediation (Appendix Two), the last of which was to be completed by all financial institutions by June 20, 1999.[36]

In early 1999 it was reported that 50–60 percent of the development fund of ordinary banks was being directed toward the Y2K problem.[37] About one-third of the banks used packaged software from the two largest providers, Diasoft and R-Style, both of which certified their packages compliant.[38]

The Central Bank reported in August, 1999 that 268 banking organizations, including 17 banks that are among the fifty largest and 14 regional banks, had either not presented the necessary data or had stated that they had not fulfilled the fourth stage of remediation, in which the results of remediation work is verified and integrated testing with external systems is carried out (Appendix Two). Assets of these organizations comprised 21.7 percent of all assets of functioning banking organizations in Russia. In nine regions the assets of banks not fulfilling stage four comprised more than 50 percent of the assets in the region. A Central Bank letter of August 17, 1999 outlines a series of measures to be taken for organizations that cannot show themselves to be compliant, including replacing computerized operations with manual ones and replacing chief executives.[39] Yeltsin's June 17th governmental order gives the Central Bank the power to withdraw licenses of banks that cannot show themselves to be compliant.[40] This August 1999 report stated that 80 percent of banking institutions have finished all four stages (Appendix Two). The press picked up on this in September, with some highlighting the negatives aspects of 20 percent not ready,[41] and others emphasizing the positive aspects of 80 percent ready.[42] This does seem like a rather large improvement in comparison with the state of affairs in May 1999, when only 10 percent of systems in the finance sector had been renovated or put into operation (Appendix One).

The banking sector is one of the few that has begun to carry out larger scale testing. A test of the Automated System of Banking Calculations of the Moscow Region (ASBR-Moskva) was carried out on July 28–30, 1999. According to the list of participants, this involved 24 Bank of Russia organizations and 455 other organizations in Moscow and Moscow Oblast. 449 of 800 registered users of the system exchanged 38,500 documents, and showed their readiness for Y2K. Nothing is said about the 351 organizations that did not take part in the test.[43] An intensive test is planned on October 9, 1999 for all banks associated with the Central Bank to exchange documents as if it were February 29, 2000.[44]

Russia's banking sector hardly has had a reputation for efficiency. Even if some operations have to be switched over to manual processing for a time, the net effects are not likely to be particularly visible in comparison with much more dramatic economic processes.

The Telecommunications Sector

The telecommunications sector in Russia comprises the general telephone network, specialized networks run by ministries and departments, and newer networks, created with Western firms that provided enhanced internal and external services. It is fairly safe to assume that Western firms who, with Russian partners, provide long distance and more advanced networking services, have the Y2K problem well in hand. Sovintel, for example, said that it completed Y2K remediation work in August, 1999.[45] Global One (Sprint) reported that testing and modernization of its network was completed in June 1999, with all remaining work to be finished by August 1999.[46] Mobile phone operator VimpelCom planned to finish remediation work by October,[47] while Comstar promised that everything would work on January 1, 2000.[48] The specialized network of the Russian Trade System was tested and said to have no Y2K problems.[49]

However, the situation may be different for the specialized networks and the general-purpose network overseen by the holding firm Svyaz'invest. Work also got off to a late start.

In late 1998 only a few of the more than 3,000 companies in the Russia telecommunications sphere had realized the importance of Y2K. Rostelekom and Svyaz'invest started working on it only in Autumn of 1998. These systems are particularly vulnerable to the Y2K problem, as 100 percent of network control systems and 75 percent of network elements in telephone structures are date sensitive.[50]

At the end of March 1999, a decree of the State Commission on Communications examined the status of Y2K work. It reported that an inventory by Goskomsvyaz' found that 20 percent of equipment in the general purpose communications network was subject to the Y2K problem, accounting for some six million connection points. About 15–20 percent of the critical systems had been modernized or replaced by this time. It was asserted that the international and intercity phone systems would most probably work reliably after the Year 2000, but noted that the more local the system, the larger the quantity of and variations in equipment subject to the Y2K prob-

lem. Local telephone companies have probably had the hardest time getting financing.[51]

According to the May 1999 data, this sector had the largest number of critical systems at 7,017. Only 11 percent had been remediated or put into operation at that time. Goskomsvyaz' planned to remove 141 systems from service altogether (Appendix One). At the end of July 1999 the number of critical systems was increased to 10,081, only 76 systems were to be turned off, and 8,551 (85 percent) required substantial remediation.[52] At the end of July, the Federal Agency (FAPSI) began testing local telecommunications systems itself to help ensure Y2K compliance. On September 22–23, Gostelekom was to perform a test involving Rostelekom, four regions (Krasnoyarsk, Tyumen', Perm', Tver'), Moscow and Moscow oblast, for a total coverage of four time zones.[53]

For the most part these statements do not paint a comforting picture for Y2K remediation in telecommunications. Although a portion of the systems rely on older technologies that may not be date-sensitive, a huge amount of capacity has been built in the last few years that does. According to one report, it was difficult to get responses from Western providers, although eventually agreements with almost all of them were signed. Decentralization in the industry means that regional companies have chosen their own solutions, have their own relationships with various providers, and most significantly, are at various stages in their awareness of the problem. At the same time investment in new equipment, especially given outstanding debts, may be difficult. This is one industry in which hardware upgrades may be the only possible path if Y2K problems are embedded in routers, switches, etc. Hence there is a fairly high likelihood that not all of this work will be completed on time and that some telephone systems will fail on Jan. 1, 2000.

IV. LONGER TERM IMPACT ON THE RUSSIAN ECONOMY

In each of the three infrastructure sectors examined above, it is clear that the Russians have carried out a great deal of work, the work started later than it should have to guarantee everything would be completed in time, and the situation was exacerbated by delays in obtaining financing. In particular, the amounts that the government says it will allocate are consistently below those that the ministries say they absolutely must have. I expect that there will be some short-term failures in these sectors, but that they will not be serious enough to cause a visible and extended impact in the economy.

One's view of the longer term implications of potential breakdowns due to the Y2K problem depends on how one views the Russian economy in general. Regarding the economic sectors left over from Soviet times, I tend to agree with the work of Clifford Gaddy and Barry Ickes, which states that many Russian enterprises produce negative value and are kept alive as a social safety net within a barter-based "virtual economy."[54] Many of these enterprises are in the military-industrial sphere, and may well be enterprises that are still running old Soviet mainframes from the late 1980's. As many as 4,000 of these may still be in use. At the Duma hearings of November 1998 it was stated that up to $400 million would be needed to replace them. These are machines that, according to a very knowledgeable source, will stop running within 3 months of the Year 2000 because of the operating system software they must run.[55] If manual processing must then be used, this may contribute to the general level of economic inefficiency in the economy, although these managers already have a huge amount of experience in dealing with unforeseen circumstances and difficult conditions.

If Russia is able to arrange the $50 million credit mentioned above, part of these funds may go to replace these machines. One could argue that it would be better to let these systems die, perhaps precipitating deeper and more effective economic reforms. Whether or not the social safety net they provide is necessary to ensure stability is too difficult for me to judge. So one effect of the Year 2000 problem may be hastening the decline of enterprises that will require massive investments anyway to become competitive or that should be shut down anyway. Investing in new computers to shore up the old production facilities is economically perverse.

Another longer term impact may be thought of as raising the general level of economic inefficiency. Telephone outages may send people to other parts of the city to make calls. The late start and low financing of Y2K work meant that the Russian government could address the remediation only of critical systems. What of the 40–60 percent of systems that are not remediated? It will certainly be more than an inconvenience if they stop working or slowly insert incorrect data into a data base. Outside the state sector there may be small businesses that were barely able to afford a computer in the first place, use pirated software and/or software created by an organization that no longer supports it, and will not be able to spare the resources needed to upgrade hardware and buy legal software. These are the types of businesses that will suffer the most from any infrastructure disruptions that may

occur, because they function in cash and have less of a cushion against economic shocks. They may be among the 1.5 million users of the Internet, and probably make extensive use of email and faxes in their daily business. The amount of resources available to them to fix their computers depends on the overall health of the economy.

Russia is hardly spending the billions of dollars that have already been and will be spent in the West. Instead of upgrading whole systems, they may settle for patching them in any way they can. Thus the Y2K problem may cause those assets to be used longer and it will lose the economic efficiencies that may have come with upgrading. In this sense the Y2K problem also contributes to increased inefficiency in the economy.

V. POLICY IMPLICATIONS

In the last few months, public pronouncements by the Russian government about the state of readiness have become less specific, although there were directives to the State Committee for Telecommunications to complete a major audit of critical systems by August 15, 1999. It would be particularly helpful for U.S businesses that do business in Russia or have dealings with Russian companies to get a better sense of the true state of affairs. We should encourage the State Committee for Telecommunications to release complete information from the more recent audits it has done.

As a corollary, if fewer systems are remediated, Russia may serve as a particularly interesting test case to find out what the true effects of the Y2K problem were. We should encourage the Russian government to collect as much data as possible about the true effects of the problem, or to facilitate its collection by objective third parties.

U.S policy should continue to be directed toward forestalling catastrophic failures that will harm large populations inside and outside of Russia. In conjunction with Russian officials, existing US initiatives and programs should be reviewed to ensure that no critical facilities have been overlooked and to facilitate the transfer of the necessary resources to protect against catastrophic failures.

Beyond this, policy choices revolve around what kind of "silver lining" might be provided for the Russian economy in conjunction with Y2K remediation. Letting counterproductive older systems die may be an unexpected benefit of the Y2K problem provided it does not lead to social unrest. Giving help to small businesses that have no other means to carry out remediation could also be a way to provide a Y2K silver-lining along the lines of the boost some Western firms are getting. But any time we speak about the longer term impact of any policies in Russia, we have to think about how to encourage the formation of the necessary conditions for true economic reform. Many believe that the an important part of the answer is building a civil society based on the rule of law that protects business activities in a stable climate. Investment in basic institution building, such as education, may be a better long-term use of funds than supporting Y2K remediation. Without stronger fundamental institutions, the Russian economy may still be lurching along from one crisis to the next long after the Y2K problem has faded from memory.

APPENDIX ONE

Inventory of Russian Federation Government Computer Systems as of mid-May, 1999.[56]

Area	Number of systems in use	Inventory completed	Number of critical systems	Share of critical systems (%)
Other ministries	678	658	328	48.1%
Key federal authorities	706	588	335	47.5%
Telecoms	15,306	14,582	7,017	45.8%
Social support	706	647	292	41.4%
Natural Resources	1,590	1,010	439	27.6%
Energy	24,296	23,375	6,398	26.3%
Trade	837	74	182	21.7%

Security-related ministries	268	144	48	17.9%
Finance	5,197	5,184	880	16.9%
Culture	21	21	3	14.3%
Transportation	1,076	991	120	11.2%
Law				
TOTAL:	50,681	47,272	16,040	31.6%

Area	Systems to be renovated	Renovated systems	Systems to be removed	Put into Operation	Cost to fix (rubles)	Cost to fix (US dollars, rate 24/1)
Other ministries	289		14	13	460,800,000	$18,432,000
Key federal authorities	354	13	8	4	507,700,000	$20,308,000
Telecoms	6,586	432	141	323	6,054,200,000	$242,168,000
Social support	318	6		6	385,100,000	$15,404,000
Natural Resources	533	1		5	178,000,000	$7,120,000
Energy	8,215	1,388	40	1,425	2,575,200,000	$103,008,000
Trade	209			45	42,800,000	$1,712,000
Security-related ministries	48	10		10	1,558,000,000	$62,320,000
Finance	628	1		66	3,308,000,000	$132,320,000
Culture	3				4,000,000	$160,000
Transportation	564	7	1	1	1,042,800,000	$41,712,000
Law					312,500,000	$12,500,000
TOTAL:	17,747	1,858	204	1,898	16,429,000,000	$657,160,000

Area	Percent Not to Be Renovated	Percent Renovated	Percent Put into operation	Percent renovated & put into operation	Renovation cost/system	To be renovated/Critical
Other ministries	57.4%	0.0%	4.5%	4.5%	$63,779	88.7%
Key federal authorities	49.9%	3.7%	1.1%	4.8%	$57,367	105.7%
Telecoms	57.0%	6.6%	4.9%	11.5%	$36,770	93.9%
Social support	55.0%	1.9%	1.9%	3.8%	$48,440	108.9%
Natural Resources	66.5%	0.2%	0.9%	1.1%	$13,358	121.4%
Energy	66.2%	16.9%	17.3%	34.2%	$12,539	128.4%
Trade	75.0%	0.0%	21.5%	21.5%	$8,191	114.8%
Security-related ministries	82.1%	20.8%	20.8%	41.7%	$1,298,333	100.0%
Finance	87.9%	0.2%	10.5%	10.7%	$210,701	71.4%
Culture	85.7%	0.0%	0.0%	0.0%	$53,333	100.0%
Transportation	47.6%	1.2%	0.2%	1.4%	$73,957	470.0%
Law						
TOTAL:	65.0%	10.5%	10.7%	21.2%	$37,029	110.6%

APPENDIX TWO

Bank of Russia Planned Stages for Y2K

Remediation in Banking Organizations[57]

STAGE	Particulars of the Stage	To be fulfilled by
1	Designate person responsible for the Y2K work Carry out inventory and prepare List of systems that may be subject to the Y2K problem	10/20/98
2	Work out plans for modernization and testing of systems, software, and hardware included in the List Define the possible executors of the work (if necessary recruit third-party organizations or specialists)	11/15/98
3	Carry out the practical modernization of systems, software and hardware in accordance with the developed plans Test systems included in the List but not requiring modernization work Develop "Emergency Plans" (plans for realizing alternative approaches if impossible to fulfill the planned tasks)	3/15/99
4	Verify results of modernization, testing equipment and systems Integrated testing of systems in conjunction with external systems Preparation and presentation to territorial institutions of the Bank of Russia Prepare a document: "Conclusion about the results of the preparation of computer systems of the banking organization (and its filials) to operating in the year 2000"	6/20/99

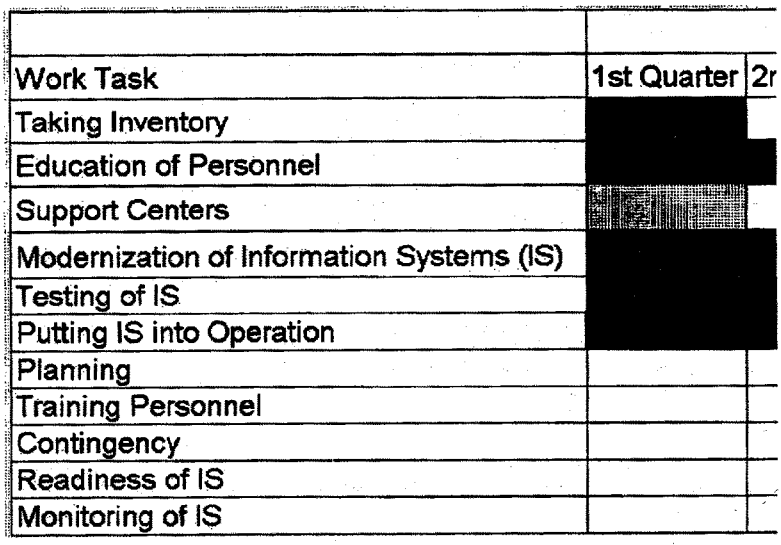
APPENDIX THREE:

Indicators for the Russian Energy System (July, 1999)[58]

	Type of Information System						
Territory	**Grid control**	**Management Information Systems**	**Systems for Monitoring energy use**	**Process Control at stations and substations**	**Program-controlled communications systems**	**Other**	**Total**
Center	131	297	58	40	71	250	847
Ural	79	170	50	13	65	28	405
North-West	67	124	32	13	26	105	367
Volga	52	126	39	23	30	1	271
North Caucasus	34	93	5	2	11	8	153
Siberia	36	171	14	12	56	11	300
East	20	92	11	5	45	12	185
TOTAL	419	1073	209	108	304	415	2528

	NUMBER	PERCENT
Total Systems, including	2,541	

Those inventoried	2,541		100.0%
Those that are found to be critical	1,575		62.0%
Systems needing modernization	1,685		66.3%
Systems modernized	467		18.4%
Systems taken out of service, replaced with manual control	2		0.1%
Modernized systems put into service	358		14.1%
	RUBLES	DOLLARS	PERCENT
General size of expenditures, including	729,500,000	$30,395,833	
for software expended	47,000,000	$1,958,333	6.4%
for software needed	288,800,000	$12,033,333	39.6%
for software expended	98,300,000	$4,095,833	13.5%
for hardware needed	295,400,000	$12,308,333	40.5%



Graph of Planned Work for Russian Unified Energy System

[11] McHenry, W. "Soviet Computing: Impasse or Opportunity?" *International Information Systems*, 1, 2, 1992, pp. 126-141. Goodman, S.E., McHenry, W.K., "The Soviet Computing Industry: A Tale of Two Sectors," *Communications ofihe ACM* 34, 6 (June, 1991), pp. 25-29.McHenry, W.K., "Computer Networks and the Soviet Style Information Society," chapter in *The Future Information Revolutionin the USSR*, edited by Richard F. Staar, New York: Crane, Russak and Co., 1988, pp. 85-114. McHenry, W.K., "The Integration of Management Information Sys-tems in Soviet Enterprises," in *Gorbachev's Economic Plans, Volume 2*, John Hardt, editor, Con-gress of the United States Joint Economic Committee, 1987, pp. 185-199. McHenry, W.K., Goodman, S.E., "MIS in USSR Industrial Enterprises: The Limits of Reform from Above." *Communications of the ACM*29, 11 (Nov., 1986), pp. 1034-1043.

[2]*Finding Common Ground: U.S. Export Controls in a Changed Global Environment*, (1991) Washington D.C.: National Academy of Sciences Press.*Global Trends in Computer Technology and Their Impact on Export Control*, (1998) National Academy of Sciences Committee to Study International Developments in Computer Science and Technology, Washington DC: National Academy of Sciences Press.

[3] McHenry, W. (1999) *The Year 2000 Problem in Russia*. Unpublished Mitre Corporation Report, 210 pages, Mar. 2, 1999. McHenry, W., Malkov, L. (1999, Aug.) "The Russian Federation's Y2K Policy: Too Little, Too Late?" *Communications of theAIS*, Vol. 2, Article 10, http://www.msb.edu/faculty/mchenryw/personal/pubs/cais.htm , current September 25, 1999. Part of my research on this topic included interviews with information systems managers in St. Petersburg, Russia in Dec. 1998, through the Baltic University of Ecology, Politics, and Law.

[4] Central Intelligence Agency (1999). *The World Factbook 1999*. Russia. http://www.odci.gov/cia/publications/factbook/rs.html , Current September 26, 1999.

[5] RAO EES Rossii. (1999, Aug. 24). "The degree of readiness of the enterprises of RAO EES Rossii for the fall-winter season of 1999-2000 for fuel oil is 60%." (In Russian) http://www.eesros.elektra.ru/ru/news/pr/show.asp?pr240899.htm , Current September 27, 1999.

[6] ComputerWorld Russia (1998). "Around the World in Bytes." (in Russian),http://www.osp.ru/cw/1998/44/00.htm , Current September 27, 1999.

[7] Elizov, V.V. (1998, Nov. 24) "Testimony." Transcript of Parliamentary Hearings on the Year 2000 Computer Problem and the Functioning of Information Systems, Nov. 24, 1998. (in Russian) http://y2k.fcsm.ru/Official/Doc_Duma/ps241198.html , Current September 26, 1999.

[8] Federal Commission for Securities of Russia. (1999, Feb. 17) "Users of illegal computer programs in state structures of the Russian federation risk coming up against the Y2K problem," (In Russian) Year 2000 Problem: News, http://y2k.fcsm.ru/Education/News/9902/990217_1.html , Current September 26, 1999.

[9] USAID Y2K Resource Center. (1999, May 10). "By the end of 1999 one-third of governmental information systems will be subject to mandatory correction," (in Russian) *News*. http://www.y2kresourcecenter.ru/ru/2/get.asp?95 , Current September 25, 1999.

[10] Federal Commission for Securities of Russia (1999, July 28) "Every Fifth Computer In Russian Federation State Structures May Produce Errors In The Year 2000" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9907/990728_2.html , Current July 30, 1999.

[11] McHenry and Malkov, 1999, *op. cit.*

[12]*Ibid.*

[13] USAID Y2K Resource Center (1999, May 10). "By the end of 1999 one-third of governmental information systems will be subject to mandatory correction," (in Russian) *News*. http://www.y2kresourcecenter.ru/ru/2/get.asp?95 , Current September 25, 1999.

[14] Federal Commission for Securities of Russia (1999, June 2) "The Pace of Fixing the Y2K Problem in Russia May Slow Down" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9906/990602_1.html , Current June 5, 1999.

[15] Gazeta.ru (1999, July 12) "Klebanov Will Report Weekly On Y2K Problem" (in Russian)*Daily News* http://www.GAZETA.ru/daynews/12-07-1999/502000_Printed.htm , Current July 27, 1999.

[16] USAID Y2K Resource Center. (1999, Sept. 23) "State Duma has passed in the third, final reading a law that will allow to channel up to $ 80 mln. to Y2K mitigation." (in Russian) *News*. http://www.y2kresourcecenter.ru/en/2/get.asp?453 , current September 25, 1999.

[17] USAID Y2K Resource Center. (1999, Sept. 23) "Government of the Russian federation intends to attract foreign credits for the sum of $50 million for solving the Year 2000 problem." (in Russian) *News*.

http://www.y2kresourcecenter.ru/ru/2/get.asp?452 , Current September 26, 1999. In order for this to happen the Minister o Economics and Vneshekonombank will hold talks to get the credits, and the Ministry of Trade will oversee commercial conditions. It is possible some of this work has already been completed, because a purchase of this magnitude has been discussed for some time.

[18] Private communication by E-Mail, September 24, 1999.

[19] McHenry and Malkov, 1999, *op. cit.* McHenry, 1999, *op. cit.*

[20] At the Kola Peninsula plant, for example, a commission examined Y2K readiness on September 15-17, including a representative from Pacific Northwest Laboratories (funded by the US DOE). The commission concluded that a large amount of work has been done and that the safety equipment at the plant is not subject to the Year 2000 problem. Similar visits are taking place to other plants. See Unattributed article. (1999, Sept. 17) "NetSL helped to solve the Year 2000 Problem at the Kolsk atomic energy plant." (in Russian) *Seti i Systemy Svyazi Online.* http://ccc.ru/news/depot/view.html?sep/1999092407 , Current September 26, 1999.

[21] USAID Y2K Resource Center. (May 15, 1999). "Solution of the Problem in Telecommunications of RAO EES" (in Russian) http://www.y2kresourcecenter.ru/ru/5/5/3/get.asp?26 , Current September
26, 1999.

[22] RAO EES (June 7, 1999). "RAO EES plans by October 1999 to replace 17 thousand computers." (in Russian) http://www.rao-ees.elektra.ru/ru/news/pub_uesr/show.asp?interfax070699.htm , Current September 27, 1999.

[23] I visited the Leningrad energy administration (Lenenergo) in December, 1998, and was told that very little on the operational side depended on digital computers, and that this situation was similar in other places in Russia. I suspect the team I spoke with either a) had not completed enough of an inventory to say anything, or b) was not being forthcoming. They did expect potential trouble from not being able to collect bills if they did not finish remediation in time, and they stated that raising tariffs to cover costs would not be politically feasible.

[24] RAO EES. (July 7, 1999). RAO EES Rossii Year 2000 Problem (as of July 1999). Presentation at USAID Y2K Resource Center. (in Russian)http://www.y2kresourcecenter.ru/ru/files/23.pdf , Current September 26, 1999.

[25] Federal Commission for Securities of Russia. (July 8, 1999) "TEK Russia will spend 2.3 Billion rubles on solving Y2K," (in Russian), *Year 2000 Problem: News,*
http://y2k.fcsm.ru/Education/News/9907/990708_1.html , Current September 26, 1999.

[26] LUKOIL (April 2, 1999). "OAO LUKOIL is successfully solving the Y2K problem." Press Release. http://www.Lukoil.ru/news/press-releases-99/04_april/02_04_1999.html , Current September 26, 1999.

[27] "Denis Kirillov describes Y2K status in YUKOS oil company. (in Russian) *For the Director of Information Department. Computer World Russia*, No. 2, Feb., 1999, http://koi.www.osp.ru/cw/cio/1999/02/03.htm , Current September 26, 1999.

[28] OAO Yuganskneftegaz. (date not provided) "Expansion of the information systems development department." (in Russian)http://www.yungisc.com/orisexpru.htm , Current September 26, 1999.

[29] Prime TASS. (February 9, 1999). "Gazprom has completely solved the Y2K Problem in computer networks, final corrections are planned for September." (in Russian)BIT No. 6 (119). http://www.prime-tass.ru/free/bit/2000/00008.htm , Current September 25, 1999.

[30] USAID Y2K Resource Center. (May 15, 1999). "Solution of the Problem in Telecommunications of Gazprom." (in Russian), http://www.y2kresourcecenter.ru/ru/5/5/3/get.asp?36 ,

Current September 26, 1999.
[31] USAID Y2K Resource Center. (July 7-8, 1999). "Abstract of a presentation of the head of the Administration of automation, informatics and measurement of the OAO Gazprom at the

international seminar 'About the state of work on solving the Y2K Problem in OAO

Gazprom.'" (in Russian), http://www.y2kresourcecenter.ru/ru/files/35.pdf., Current September 26, 1999.
[32] Prime Tass (August 17, 1999). "Gazprom plans in September to finish work on modification of systems for resolving the Y2K Problem," (in Russian) Moscow, BIT No. 31 (144). http://www.prime-tass.ru/Free/Bit/2000/a0095.htm., Current September 25, 1999.

[33] USAID Y2K Resource Center. (July 7-8, 1999). "Abstract of a presentation of the head of the Administration of automation, informatics and measurement of the OAO Gazprom at the

international seminar 'About the state of work on solving the Y2K Problem in OAO

Gazprom.'" (in Russian), http://www.y2kresourcecenter.ru/ru/files/35.pdf., Current September 26, 1999.
[34]*ComputerWorld Russia* #48, 1997.

[35]*St. Petersburg Business News: Financial News*, February 8, 1999 # 4 (294) (*Kommersant* Feb 2, 1999).

[36] Kozlov, A.A. Bank of Russia (1998, September 28). Order of the Bank of Russia No. 362-U. About measures for oversight of fulfillment of work on the Year 2000 Problem. (in Russian) http://www.cbr.ru/publications/362-u.htm., Current September 26, 1999.

[37] Federal Commission for Securities of Russia (Feb. 17, 1999). "50-60% of the development funds of the average Russian bank are allocated to solve Y2K problem, says Yu. Koval, Deputy Chairman ofAutobank's Board." (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9902/990217_6.html., Current September 26, 1999.

[38] McHenry, 1999, *op. cit.*

[39] Goryunov, V.N. (August 16, 1999). Central Bank of Russia Letter. About Fulfillment of Work in Conjunction with Order of the Bank No. 362-U. (in Russian) http://www.cbr.ru/publications/244_t.htm., Current September 26, 1999.

[40] Yeltsin, B. (1999, June 17) Decree Of The President Of The Russian Federation. About Measures That Cannot Be P Off To Solve The Y2K Problem In The Russian Federation No. 194-RP (in Russian), http://www.algo.ru/law2000/laws/president.asp., Current July 1, 1999.

[41] RosBiznesKonsalting. "Main Administration of the Bank of Russia for Moscow believes that in conjunction with the Y2K Problem, breakdowns are possible in the operation of 20% of banks." (in Russian) *Russiya-on-layn, Novosti RBK*, http://www.roline.ru/rbcnews/16.09.1999/937469464+29742.rhtml., Current September 26, 1999.

[42] USAID Y2K Resource Center. "Banking system of Russia is preparing for the arrival of 2000. Several articles, appearing in the central press, and a seminar of the Central Bank of September 16, became sources of encouraging information." (in Russian). *News*. http://www.y2kresourcecenter.ru/ru/2/get.asp?419., Current September 26, 1999.

[43]Central Bank of Russia (1999, August 30). Information. (in Russian) http://www.cbr.ru/publications/990830_1457_Asbr.htm., Current September 26, 1999. Participants are listed at http://www.cbr.ru/publications/spisok.htm., Current September 26, 1999.

[44] USAID Y2K Resource Center. "Banking system of Russia is preparing for the arrival of 2000. Several articles, appearing in the central press, and a seminar of the Central Bank of September 16, became sources of encouraging information." (in Russian). *News*. http://www.y2kresourcecenter.ru/ru/2/get.asp?419., Current September 26, 1999.

[45] Sovintel (September, 1999). Sovintel Network. Status of the project. GlobalOne (in Russian) http://www.sovintel.ru/rus/y2k/4.html., Current September 27, 1999.

[46] GlobalOne. (August, 1999). The Year 2000 Problem. Status of the P-2000 Project of GlobalOne (in Russian). http://www.global-one.ru/y2k/status.htm., Current September 27, 1999.

[47] Beeline. (1999). getting 2000-year ready. http://www.beeline.ru/About/Y2K_e.html., Current September 27, 1999.

[48] Comstar. (1999). Program Y2000 (in Russian). http://www.comstar.ru/project/tech/y2000.html., Current September 27, 1999.

[49] Russian Trade System. (March 26, 1999). Carrying out of testing of the telecommunications network in solving the

Year 2000 problem -- experience of the Russian Trade System (in Russian). http://www.rtsnet.ru/tc/news/2problem990326.htm , Current September 26, 1999.

[50] Chasin, Petr (1999, Jan. 26-Feb. 1) "Then it will be too late." *PC Week*, # 2 (176)http://www.pcweek.ru/Year1999/N2/cp1251/Communications/chapt2.htm .

[51] USAID Y2K Resource Center. (March 31, 1999). "Materials of GKES." (in Russian) http://www.y2kresourcecenter.ru/ru/5/5/3/get.asp?29 , Current September 27, 1999.

[52] Federal Commission for Securities of Russia (1999, July 28) "Every Fifth Computer In Russian Federation State Structures May Produce Errors In The Year 2000" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9907/990728_2.html , Current July 30, 1999.

[53] USAID Y2K Resource Center. (September 23, 1999). "Today an inter-regional test for communications operators for the Y2K problem is being completed which was organized by Gostelekom for September 21-23." (in Russian) http://www.y2kresourcecenter.ru/ru/2/get.asp?451 , Current September 27, 1999.

[54] Gaddy, Clifford, Ickes, Barry, "This Bailout Will Set the Stage for the Next Crisis," *The Los Angeles Times*, July 17, 1998, http://www.brook.edu/views/op-ed/gaddy/19980717.htm , Current September 26, 1999.

[55] McHenry and Malkov, 1999, *op. cit.*

[56] USAID Y2K Resource Center, News. (1999, May 10). "By the end of 1999 one-third of governmental information systems will be subject to mandatory correction," (in Russian) http://www.y2kresourcecenter.ru/ru/2/get.asp?95 , Current September 25, 1999.

[57] Kozlov, A.A. Bank of Russia (1998, September 28). Order of the Bank of Russia No. 362-U. About measures for oversight of fulfillment of work on the Year 2000 Problem. (in Russian) http://www.cbr.ru/publications/362-u.htm , Current September 26, 1999.

[58] RAO EES. (July 7, 1999). RAO EES Rossii Year 2000 Problem (as of July 1999). Presentation at USAID Y2K Resource Center. http://www.y2kresourcecenter.ru/ru/files/23.pdf , Current September 26, 1999.

PREPARED STATEMENT OF DR. EDWARD WARNER III

Introduction

Thank you Mr. Chairman and members of the Committee. I am very pleased to be here this morning, and welcome the opportunity to discuss the Department of Defense's cooperative efforts with the Russian Federation on the Year 2000 problem. The Department particularly appreciates the interest that this Committee has taken throughout our engagement with the Russian Federation on our Y2K efforts, and the continuing support for this endeavor from the members and staff.

Background

Our first substantive Y2K discussions with the Russian Ministry of Defense (MoD) were held this past February on the margins of the Defense Consultative Group (DCG). At the conclusion of the DCG I exchanged a letter with my co-chairman Colonel General Valerly Manilov, the First Deputy Chief of the Russian General Staff, inviting the MoD to continue discussions of a range of possible Y2K cooperative activities in Washington DC in the spring. Unfortunately the crisis in the Balkans intervened, and the strained relations between our nations over the conflict in Kosovo resulted in cancellation of the scheduled April session. But it was clear to me when I met with General Manilov in mid-August, and clear to our DoD participants when the working groups from each side reconvened at the end of the month, that during the pause in discussions, the MoD had continued work, as did the US, on the three goals of cooperative Y2K engagement agreed to in February: (1) sharing Y2K management experiences; (2) developing specific procedures to manage the Y2K transition period together; and (3) addressing Y2K challenges associated with ensuring the security, reliability, and control of nuclear weapons and materials. And so, while the loss of time was regrettable, especially since we face an unmovable deadline, both the US and the Russian Federation were poised for rapid reengagement, and we are moving out aggressively to implement the initiatives I will discuss today.

As with all of DoD's Y2K work, we approached our engagement with Russia not only from the perspective of "fixing" Y2K computer problems and preparing to manage the consequences of possible Y2K failures, but with an eye towards improving our bilateral defense cooperative with Russia. In developing specific initiatives to meet the goals listed above, we sought to leverage the experience and resources of established programs, and use Y2K as an opportunity to develop additional avenues for the continued improvement and stabilization of relations between both nations.

The result is an integrated program involving cooperation in five areas: (1) The Center for Year 2000 Strategic Stability; (2) Nuclear stockpile security; (3) Nuclear command and control; (4) Secure "hotline" communications; and (5) Information technology management. To date, we have reengaged with the Russian Federation on all of these areas except nuclear command and control, and I expect reengagement on that issue to begin next month.

Today, I will discuss our progress in establishing the Center for Y2K Strategic Stability, nuclear stockpile security, assured communications, and overall Y2K Management.

Center for Year 2000 Strategic Stability

I'll start with the Center for Year 2000 Strategic Stability. This effort has certainly received the bulk of the media attention to date, and I know that it is an item of particular interest to several of you. As you know, on 13 September in Moscow, Secretary Cohen and Minister Sergeyev signed a joint statement declaring the intent of the US and Russia to establish the Center for Year 2000 Strategic Stability. The Center, to be located on Peterson Air Force Base in Colorado Springs, will provide a venue for sharing missile launch detection information collected by US sensors across the year 2000 date change. In the Center, US and Russian military personnel will sit side by side during the millennium transition period and continuously monitor US-provided information on missile and space launches. US personnel will be in voice contact with operators in the North American Air Defense Command, and Russian personnel will be in voice contact over highly reliable secure communications lines with a command center in Moscow. In addition to monitoring possible missile launches, the Center will provide a direct means for consultations regarding other defense-related problems that emerge over the Y2K transition period.

Construction of the center is on schedule, with a projected completion date of 1 December. We continued to work out details of the operations concept for this center with our Russian counterparts when they visited the facility in Colorado Springs last week. We are awaiting final agreement with Moscow, but generally speaking, the Center will open for training in late December, and will operate 24 hours a day, 7 days a week, through the opening week or two in January.

Let me stress that experts in both countries agree that the likelihood of Y2K failures in computer systems associated with our nuclear weapons, supporting command and control, and early warning systems is extremely remote. Moreover, sufficient safeguards are in place to protect against the consequences of such failures. Nonetheless, we are mindful of concerns by some that a Y2K induced failure could result in the accidental launch of nuclear weapons, and of the potentially severe consequences of any misinterpretation of early warning information. We have a responsibility to provide the American people with every assurance that such accidents will not occur. The Center can allay the concerns of the public, and provide additional safeguards appropriate to this period of heightened uncertainty. As such, the Center is a Y2K application in the spirit of many risk reduction practices developed over the years by the US and Russia to prevent apparent anomalies in military activities from turning into serious incidents.

The Center for Year 2000 Strategic Stability being set up in Colorado Springs is not a replacement for the permanent Joint US-Russian Warning Center currently under negotiation that is slated to be established in Moscow. At the Moscow Summit in September 1998, Presidents Clinton and Yeltsin agreed to the *reciprocal* sharing of early warning date of a threat by both sides of the launches of ballistic missiles and space vehicles. The Center is a temporary measure, and will display US data only. The permanent Joint Warning Center will provide side by side displays of data derived from each nation's early warning satellites and radars. We will meet with the Russian Federation next month to continue discussions on implementation of the long-term shared early warning initiative.

Nuclear Stockpile Security

The security of nuclear materials is another critical issue that requires special attention in connection with the Year 2000 transition. For several years DoD, through the Nunn-Lugar Cooperative Threat Reduction (CTR) program administered by the Defense Threat Reduction Agency (DTRA), has pursued programs for improving the management of nuclear weapons storage sites throughout Russia. Last December DTRA expanded its efforts, and initiated discussions focused on the continuous safe and secure storage, transport and accounting of these weapons of mass destruction (WMD) across the period of Y2K vulnerability.

In March, DTRA continued its Y2K discussions with the 12th Main Directorate of the MoD, which is responsible for the storage and security of all non-deployed Russian nuclear warheads. Of special concern are the security systems in nuclear storage sites affecting access control, perimeter monitoring, fire detection and sup-

pression, and warhead inventory and accountability. At that meeting, representatives from the MoD confirmed that there had been no evaluation of computers associated with the physical security and inventory management systems for Y2K vulnerability. MoD welcomed any assistance DoD could offer in this regard.

When DTRA renewed discussions with the MoD in August, it was evident that substantial progress had been made in the intervening 5 months in the assessment of, and planning for, possible Y2K disruptions associated with nuclear stockpile safety and security. The 12th Main Directorate has embarked on a credible and focused plan to monitor computer systems that support nuclear storage and security during the Y2K rollover. This represents a significant and positive change in posture since our previous discussions of Y2K vulnerabilities and consequences in March. Beginning in December 1999 and lasting through March 2000, the Russians will maintain a special Y2K monitoring and control center at each of their 50 main nuclear storage sites. The centers will operate around the clock, staffed by specially selected and trained soldiers. The centers will monitor key systems, to include those linked to physical security; power, water and telecommunications infrastructure; and the microenvironments within the warhead storage areas.

In conjunction with its planning for the monitoring regime, the 12th Main Directorate has also conducted a comprehensive readiness assessment of its response capabilities. Unfortunately, the result of this assessment has revealed significant shortfalls in the ability to respond in a timely and effective manner to security or safety disruptions that the monitoring centers might detect. Within the monitoring centers, the lack of standard equipment such as personal computers and faxes could readily produce delays in the decision process. Once decisions are made, the ability to respond appropriately will be compromised by equipment that is unreliable, obsolete, or in disrepair.

As an outgrowth of our two meetings with the 12th Main Directorate in August, the Russian Federation has submitted a written request to DoD for equipment to assist in consequence management of potential Y2K events. Equipment requested would cost approximately $15.5M; specific items include emergency generators, fire trucks, warhead handling and medical response vehicles, radios for security response forces and field reporting, and back-up communications capabilities.

DoD has reviewed the Russian request, and agrees that the types of equipment and quantities requested make sense. Furthermore, we have assessed this Y2K submission relative to types and quantities of equipment already requested and planned for transfer to Russia under longer term CTR initiatives, and have determined that most of the items—$13M of the $15.5M—fall clearly within the scope and purpose of the CTR program. The bulk of the requirement for Y2K is a simple and straightforward request to accelerate and amplify the assistance that is already being provided or has been planned through the existing Nunn-Lugar program.

DoD is moving quickly to identify funding options for this request. There is very little available under prior year CTR funding, and FY00 CTR funds are on hold pending Russia's recertification for the program. However, we have identified approximately $3 million from the CTR program and the DoD Y2K Supplemental to pay for the elements of the Russian request that we deem demand the highest priority. The majority of these funds will be used to purchase computers, radio sets, and other automation equipment that will assist the Russians in maintaining the security and accountability of their stockpile in the face of the Y2K challenge. We will be meeting with the Russians in early October to discuss this issue and seek mutual agreement on the priorities we have set.

Assured "Hotline" Communications

Assured communications between US and Russian leaders is a priority at all times, and of particular concern over the millennium date change. There are seven direct communication links, or "hotlines," between Russia and the United States to guarantee our leaders immediate communication with one another when necessary. Among these are the direct links between our Presidents, the foreign affairs link between the Secretary of State and Minister of Foreign Affairs, and the hotline connecting each country's Nuclear Risk Reduction Centers. In addition, reliable secure communications will be essential for the operations of the temporary Center for Y2K Strategic Stability.

Communications experts from the US and Russia nations started discussions concerning the Year 2000 problem last October. These discussions were continued during the week of 15 February, when representatives from the Defense Information Systems Agency, White House Communications Agency, Army, Joint Staff, and Department of State met with their counterparts from the Ministry of Defense and Ministry of Communications in Moscow. Despite events in Kosovo, our communications experts were able to sustain contact during the spring, and during that time Y2K problems were identified at the Russian ground station, and in commercial

software on both sides, which would prevent full operation of six of the seven direct communication links over the Y2K transition.

When talks resumed in August, the Russian Federation agreed with US recommendations regarding Y2K vulnerabilities in the current hotline architecture, and the US agreed to provide the Russian Federation with Y2K compliant software and computer workstations to correct program deficiencies in outage reporting, monitoring, and channel reroute operations. Procurement actions for this equipment have been initiated, and while the schedule is tight we are confident that the fixes will be installed and tested by December. The August discussions also addressed possible contingency measures, to include implementation of backup analog circuits, additional secure phone/facsimile capability, and installation of emergency INMARSAT devices on both sides. Finalization of Y2K operational and contingency planning for secure communications will occur at the US-Russia technical experts group meeting scheduled for 18–22 October.

Information Technology Management

While building on existing relationships for addressing nuclear systems and communications issues, DoD is also pursuing a new initiative with MoD in the area of information technology management. In the US, the Year 2000 problem has presented new and unique information technology challenges. We have learned a great deal, both through our own successes and missteps to date, and through the information we have exchanged with our Allies over the past year. Throughout the Federal government, there is a consensus among Chief Information Officers that the Y2K experience will fundamentally change the way that we manage information technology in the future. When our technical experts met with MoD last month, we learned that they have reached the same conclusion.

The Y2K discussions in August provided DoD with our first real insight into the MoD's approach to Y2K assessment, remediation, and containment. Taking a functional approach to system definition—and learning from DoD's mistake in this regard—MoD has identified 1000 total computer-based systems, with approximately 100 systems defined as mission critical. I would note that with this functionally based definition, a single computer can constitute a system, while an entire aircraft can be defined as a single system. MoD is responding to Y2K problems in its mission critical systems through a combined approach of retirement, remediation, and encapsulation, depending on the nature of the problem and complexity of potential solutions. MoD is bypassing the type of individual system certification and integration testing that characterizes much of the DoD test regime, and is moving directly into operational testing of its mission critical systems.

I think it is important to note at this point that there is no single right or wrong way to fix Y2K problems. This is a complicated enterprise, and the best solution for a particular department or nation is a function of time, resources, criticality, and engineering discipline. The fact that the Russian MoD is following a different protocol and timetable for addressing its Y2K problem does not man that approach is deficient—it just means that its different. We emerged from our discussions convinced that the MoD is treating its Y2K problem very seriously, and has designed and executed a program appropriate to its situation. We look forward to continuing our discussions with the MoD on Y2K and on more general information technology management issues, when the US-Russian Information Technology Management Working Group meets in Washington the week of 18 October. In response to a specific request by MoD, we plan to have representatives from major US software companies participate with us in this session.

Conclusion

In conclusion, I would note that, despite the time lost due to the Kosovo conflict, our cooperative Y2K activities with the Russian Federation defense establishment will make a significant contribution to both nations as we transit into the next millennium. The dedication of participants on both sides has helped us to make up for the lost time rapidly. I am convinced that each of the efforts I've discussed is making a long-term contribution to enhanced military-to-military relationships and strategic stability. We will continue to work closely with the President's Council for Year 2000 Conversion as we pursue these efforts, and will keep this committee apprised of our progress.

○