Y2K: A THREAT TO U.S. INTERESTS ABROAD?

HEARING

BEFORE THE

COMMITTEE ON INTERNATIONAL RELATIONS HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

THURSDAY, OCTOBER 21, 1999

Serial No. 106–92

Printed for the use of the Committee on International Relations

U.S. GOVERNMENT PRINTING OFFICE
63–868 CC WASHINGTON : 2000

COMMITTEE ON INTERNATIONAL RELATIONS

BENJAMIN A. GILMAN, New York, *Chairman*

WILLIAM F. GOODLING, Pennsylvania
JAMES A. LEACH, Iowa
HENRY J. HYDE, Illinois
DOUG BEREUTER, Nebraska
CHRISTOPHER H. SMITH, New Jersey
DAN BURTON, Indiana
ELTON GALLEGLY, California
ILEANA ROS-LEHTINEN, Florida
CASS BALLENGER, North Carolina
DANA ROHRABACHER, California
DONALD A. MANZULLO, Illinois
EDWARD R. ROYCE, California
PETER T. KING, New York
STEVE CHABOT, Ohio
MARSHALL "MARK" SANFORD, South Carolina
MATT SALMON, Arizona
AMO HOUGHTON, New York
TOM CAMPBELL, California
JOHN M. McHUGH, New York
KEVIN BRADY, Texas
RICHARD BURR, North Carolina
PAUL E. GILLMOR, Ohio
GEORGE RADANOVICH, California
JOHN COOKSEY, Louisiana
THOMAS G. TANCREDO, Colorado

SAM GEJDENSON, Connecticut
TOM LANTOS, California
HOWARD L. BERMAN, California
GARY L. ACKERMAN, New York
ENI F.H. FALEOMAVAEGA, American Samoa
MATTHEW G. MARTINEZ, California
DONALD M. PAYNE, New Jersey
ROBERT MENENDEZ, New Jersey
SHERROD BROWN, Ohio
CYNTHIA A. McKINNEY, Georgia
ALCEE L. HASTINGS, Florida
PAT DANNER, Missouri
EARL F. HILLIARD, Alabama
BRAD SHERMAN, California
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey
JIM DAVIS, Florida
EARL POMEROY, North Dakota
WILLIAM D. DELAHUNT, Massachusetts
GREGORY W. MEEKS, New York
BARBARA LEE, California
JOSEPH CROWLEY, New York
JOSEPH M. HOEFFEL, Pennsylvania

RICHARD J. GARON, *Chief of Staff*
KATHLEEN BERTELSEN MOAZED, *Democratic Chief of Staff*
RONALD C. CRUMP, *Counsel*
MARILYN C. OWEN, *Staff Associate*

CONTENTS

WITNESSES

APPENDIX

Prepared statements:

Additional material:

Y2K: A THREAT TO U.S. INTERESTS ABROAD?

House of Representatives,

COMMITTEE ON INTERNATIONAL RELATIONS,
WASHINGTON, D.C.

The Committee met, pursuant to notice, at 10:07 a.m. In Room 2172, Rayburn House Office Building, Hon. Benjamin A. Gilman (Chairman of the Committee) Presiding.

Chairman GILMAN. The Committee on International Relations will come to order.

Our Committee on International Relations has engaged in a comprehensive oversight of a number of issues affecting the foreign interests of our Nation and on the Administration's policies that identify and advance those interests.

In so doing, we have a further fiduciary duty to make certain that the agencies charged with protecting and advancing our interests are themselves in the position to do so effectively. In meeting our oversight responsibility in that regard, I have asked the U.S. General Accounting Office to do a study of the readiness of our Department of State and our Agency for International Development to meet any Y2K challenges when the year 2000 begins.

GAO was specifically requested to study three things: The first was whether the State Department, through its leadership of the President's Year 2000 Council International Relations Working Group, has an adequate strategy in place to assess and address international year 2000 risks.

Second, we wanted GAO to ascertain whether the State Department has an adequate strategy in place to ensure the safety of Americans overseas who may face risks from year 2000 failures.

Last, we need to answer the question of whether our U.S. Agency for International Development has taken the necessary appropriate steps to address with foreign nations whether year 2000 risks associated with information technology projects and systems that USAID has funded.

We are here today to hear not only their report, but just as importantly, to ascertain on the record the Administration's position and views as to its readiness for problems that may come its way because of the Y2K phenomenon. The Administration will now be on the record as to its readiness.

It is important that we press for this status report and an accounting for any state of unreadiness by either State or USAID.

Now I will invite Mr. Gejdenson, our Ranking Minority Member, to present any opening remarks that he may have.

[The prepared statement of Chairman Gilman appears in the appendix.]

Mr. GEJDENSON. Thank you, Mr. Chairman. I commend you for holding these hearings. Clearly we are going to be dealing with Y2K issues long after January 1st, particularly for Americans overseas and for American national security. We may have more work to be done on the Y2K issue in other countries than we do here at home. I have seen the reports that State and USAID are well on their way to dealing with the Y2K issues and commend both of these organizations for their efforts here.

What concerns me is whether American officials overseas will be in a position to help Americans who may find themselves in some kind of jeopardy. Whether a medical device fails overseas, whether countries overseas have failures in their cash machines, their phone systems, will American embassies have the personnel in place and the inclination to provide assistance to Americans who are in trouble.

Of course, we are concerned about nuclear power plants and military systems, ballistic missiles and weapons of mass destruction in other countries. I think one of the things we have to make sure we focus on is that American expertise and Western European expertise is available, especially, to countries of the former Soviet Union and some of the less developed countries to help these countries deal with potential disasters. I am hopeful that the witnesses today will give us some assurances in these areas, but particularly again that we will have a system in place when an American citizen shows up at an embassy, that the American embassy will be able to help them, whether it is a medical or financial emergency where the systems have not yet been adapted to deal with the Y2K crisis.

My son is now in Bolivia, and his girlfriend is in New York. She happens to live in a part of New York that has an area code that Bolivia still does not recognize. Now, he has been there for 3 months, and she can call him but he cannot call her. That is not exactly an international crisis, but if we have somebody with a medical emergency in a country where a Y2K problem has affected the ability to communicate, that could be something that we must be able to deal with.

So I hope we hear from the witnesses today on those matters.

Thank you very much.

Chairman GILMAN. Thank you, Mr. Gejdenson. This morning we have two panels of three witnesses each. The first panel consists of Mr. John O'Keefe, Special Representative for Year 2000, United States Department of State; Mr. Richard Nygard, Chief Information Office for the U.S. Agency for International Development; and Lawrence Gershwin, National Intelligence Officer for Science and Technology, Central Intelligence Agency.

The second panel consists of Ms. Jacquelyn Williams-Bridgers, Inspector General of the Department of State; Mr. Theodore Alves, Assistant Inspector General for Audits, United States Agency for International Development; and Ms. Linda Koontz, Associate Director, Accounting and Information Management Division at the U.S. General Accounting Office.

Chairman GILMAN. We welcome all of our witnesses. Mr. Nygard, you may open, but before we begin, you may put your full statement in the record and summarize. Without objection your full statement will be made a part of the record. Mr. Nygard.

Mr. NYGARD. Thank you, Mr. Chairman. I appreciate the opportunity to appear before you this morning to describe the response of USAID's to potential Y2K disruptions that may affect our agency's systems, our programs, and the countries in which we operate. As you suggested, I have submitted a written statement for the record and will summarize it here.

Chairman GILMAN. Without objection.

STATEMENT OF RICHARD C. NYGARD, CHIEF INFORMATION OFFICER, U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT

Mr. NYGARD. I will cover three main topics: The condition of our internal information systems, the steps we are taking to ensure our programs and operations will continue into 2000, and third, the work we are doing to prepare for possible humanitarian assistance early next year.

First, on our internal systems, we have a total of seven mission-critical systems, two of which have been replaced. Of the remaining five, four have been repaired and implemented. The fifth system, USAID's New Management System (NMS), is on schedule for completion at the end of this month. We are continuing to test the Y2K readiness of our other noncritical agency systems. In repairing and testing our systems, USAID's prime systems contractor has used sophisticated techniques for detailed measurement of Y2K progress and comprehensive testing.

USAID is also working with our Inspector General and our prime systems contractor to expand and improve technical discipline throughout our information systems management. One important effort in this area is documenting the results of Y2K testing. We realize the importance not only of conducting the tests but also assuring that written records permit independent verification that the testing was done. We have made significant progress and will continue to seek improvements in this area.

Second, on business continuity planning, USAID is carrying out three forms of such planning. First, formal planning for our critical internal business systems; third, program assessments to assure that ongoing USAID activities will continue after January 1st; and 3rd, external coordination with the Department of State's contingency planning at each overseas' post. Business continuity planning for our mission-critical systems focuses on critical financial functions: payments, obligations, and funds control.

Starting last fall, USAID staff, supported by contractors, analyzed financial processes and ranked the importance of each process. Next, detailed work-around techniques for the business processes were identified. Manual procedures and local spreadsheet applications were developed to facilitate interim operations if disruption to normal operations occurs.

As of October 15th, all 44 of our overseas missions that perform accounting functions for USAID reported that their rehearsals of Y2K contingency plans for core financial functions are complete and reported as successful by the mission controllers. All reported no notable startup errors when fiscal 2000 operations were commenced in early October. Documentation of these rehearsals is still in process.

Second, while USAID cannot assure that each of the countries where we operate won't be affected by Y2K disruptions, we have taken significant actions to assure program continuity after January 1st. Five percent of the fiscal 1999 development assistance and child survival funding for each of our regional bureaus was set aside to be used as necessary for Y2K Program repairs. Before the funds could be used for purposes other than Y2K, the bureau assistant administrators had to affirm that all prudent steps had been taken to make programs Y2K compliant.

The USAID Administrator met with each regional assistant administrator twice this year to discuss Y2K compliance and the continuity of mission and program operations. Heads of all bureaus indicated that necessary steps had been taken by the end of fiscal 1999 to assure continuity of program operations.

A number of actions were also taken to assist missions and programs in assuring program continuity. These included: performing independent Y2K assessments on critical infrastructure and government systems in 50 countries; training program and host country managers on Y2K methodologies; making available contingency planning consulting and workshops for embassies, missions, and host countries; cooperating with other donors such as the World Bank; participating in governmentwide international groups addressing the Y2K problem; and developing a Y2K management tool kit, which I have a copy of here, to help system managers, government planners, business owners, and community readiness leaders in the developing world. I will be prepared to talk about that more in the question session if there is a desire to do so.

Externally, we are working with the Department of State's Y2K Committee under the authority of the chief of mission at each overseas post. Embassy Y2K Committees with the participation of USAID mission staff continuously evaluate host nation Y2K readiness. To provide additional support of mission program and host country Y2K issues, we have established Y2K resource centers in Washington, Russia, Ukraine and Egypt and have developed business continuity and contingency plans at individual missions in Europe.

The third category is humanitarian assistance. I will summarize that briefly. We have taken a number of actions to ensure that we will be able to respond after the first of the year should the situation require it. We sent out a worldwide guidance cable. We have improved our communications systems internally. We have worked with our humanitarian assistance partners, PVO's and others, to ensure that they are Y2K compliant. We will keep our operations center open 24 hours a day, 7 days a week at the beginning of January. We are making sure that strategically located stockpiles of food, blankets, and emergency supplies are at capacity levels; and we are working closely with the Department of State and the Department of Defense in preparing for activities that may happen early next year.

We are concerned that the potential need for Y2K-related humanitarian aid coming on top of Kosovo, Central America, and the ongoing African crisis may exceed the capacity of USAID and other donors. We will do everything possible, but out resources are limited.

In closing, Mr. Chairman, let me repeat that we at USAID, working with our colleagues at the Department of State and other Federal agencies and partners, have made major progress in assuring that our people and our programs won't be seriously affected by Y2K. I cannot guarantee that there will be no disruptions because of the conditions in the countries where we operate, but I believe that the actions we and others have taken will provide the safety of our people and the continuity of our programs.

Chairman GILMAN. Thank you.

[The prepared statement of Mr. Nygard appears in the appendix.]

Chairman GILMAN. Our next witness is John O'Keefe, Special Representative for the Year 2000 from the United States Department of State. Mr. O'Keefe, you may summarize as you deem appropriate.

Mr. O'KEEFE. Thank you, Mr. Chairman. As you suggest, I will summarize from the full testimony and submit that full testimony for the record.

Chairman GILMAN. Without objection.

STATEMENT OF JOHN O'KEEFE, SPECIAL REPRESENTATIVE FOR THE YEAR 2000, UNITED STATES DEPARTMENT OF STATE

Mr. O'KEEFE. Those working on the Y2K problem are confronted with limited resources, limited time, imperfect information, and uncertainty regarding the scope and duration of its potential effects. Despite these difficulties, the State Department has used its existing infrastructure and experience in crisis management and diplomacy to prepare for the potential impact of Y2K problems overseas.

We have not done this alone, however. Work on the international aspects of the Y2K problem has truly been an interagency and multilateral cooperative effort as well as a public and private sector partnership.

As reflected in the State Department's Y2K preparations, one of our highest priorities is ensuring the safety of Americans living and traveling abroad, including our own employees. We have done this by focusing our Y2K efforts in three key areas.

First, we have worked to make sure that our mission-critical systems all over the world are themselves Y2K compliant so that we can continue to provide critical services to Americans overseas and domestically. The Department has fully remediated and implemented 100 percent of its mission-critical systems deployed both domestically and internationally.

Second, we have been coordinating closely with our missions abroad to assure their continued safe operation despite any potential Y2K-related disruptions in the host country infrastructure. We have taken similar backup precautions for our domestic facilities.

Third, we have conducted a dialogue and continue to cooperate with other countries to encourage their efforts to prepare for Y2K.

The Department is in the process of exercising its remediated systems to ensure that our business processes are maintained in the event of any Y2K failures.

In addition to systems readiness, our posts have taken numerous steps to assure that their core functions including the protection of American citizens, can continue uninterrupted. We have used existing emergency plans as a base and modified them to reflect some of the unique challenges posed by Y2K. Preparations overseas have followed a multiphased approach. In February 1999, all posts received a contingency planning tool kit to assist in their planning for the rollover. Then in May 1999, all chiefs of mission certified post readiness for the transition to the Year 2000 and identified resources required to ensure operational readiness. Based on this information, the Department prepared a request and received some funding for generators and fuel in addition to the funds for systems remediation.

The final critical element in the post contingency planning strategy is the contingency plan validation process. Using a web-based tool organized by post business processes, posts are consolidating previous tool kit responses, preexisting emergency planning, and guidance from the department into a standardized format for a Y2K contingency plan. By October 27th, posts will complete the contingency plan validation process.

Preparation for our domestic facilities has been equally thorough. The Department has inventoried operating equipment in all of our buildings, 23,000 items from elevators to pumps, lights, fans, and valves and verified reliability with manufacturers, with GSA, and our own experts. Our preparation to ensure the safety of Americans overseas who may face risks from Year 2000 failures has been extensive. Our efforts have focused on providing information to the public, being open about our preparation, and ensuring backups for key consular services.

The January, 1999 announcement to the public alerted traveling Americans to the Y2K phenomenon in general. It was followed in July with guidance for personal preparedness in areas such as health-related issues and noted the inability of our missions to directly provide food, water, and shelter to the millions of Americans abroad.

[The information referred to appears in the appendix.]

On September 14th, the Department issued updated consular information sheets for every country in the world. I am pleased to provide you a summary of our country by country Y2K consular information sheet. Each sheet contains a section assessing potential for disruptions, remediation efforts, and possible impact in a specific country. So our citizens are informed of potential risks.

[The information referred to appears in the appendix.]

Mr. O'KEEFE. At the end of October, we are anticipating issuing strengthened consular information sheets for a small number of countries which have not made the anticipated progress on their remediation efforts. Furthermore, if any authorized departure decisions are made for nonemergency personnel at posts, the U.S. public will be notified in the form of a travel warning immediately.

Finally, if serious disruptions occur, we will prioritize consular services to American citizens, focusing in particular on evacuations, if necessary, medical emergencies, welfare and whereabouts inquiries, and deaths. We have coordinated with other agencies regarding emergency services for Americans abroad during the rollover period.

Since time is up, I will just summarize the fact that the Department has successfully tested our reporting plan. This was the most comprehensive worldwide Y2K reporting exercise within the U.S. Government and that in the international sphere, which you noted in your opening remarks. The interagency working group on international matters is cochaired by the Department of State and the Department of Defense, and we have been meeting regularly since February 1999. It serves both to exchange information and to develop policy.

Our Members have been involved in a number of international initiatives to mitigate the potential effects on Y2K on aviation safety, ports and maritime, nuclear power plants, small- and medium-sized businesses and operational readiness of our military forces abroad.

Mr. Chairman, this concludes my testimony. Thank you for the opportunity to speak to the Committee today. I will be happy to answer any questions the Members may have.

Chairman GILMAN. Thank you, Mr. O'Keefe.

[The prepared statement of Mr. O'Keefe appears in the appendix.]

Chairman GILMAN. We now proceed to Lawrence Gershwin, National Intelligence Officer for Science and Technology at our Central Intelligence Agency.

Mr. GERSHWIN. Thank you. Mr. Chairman and Members of the Committee, I am pleased to have the opportunity today to provide the Committee with the intelligence community's latest assessment of the status of foreign preparedness for Y2K. I will submit my full statement for the record, and I will summarize the rest of it now.

Chairman GILMAN. Without objection.

STATEMENT OF LAWRENCE K. GERSHWIN, NATIONAL INTELLIGENCE OFFICER FOR SCIENCE AND TECHNOLOGY, CENTRAL INTELLIGENCE AGENCY

Mr. GERSHWIN. Our assessment is essentially a snapshot of the current state of international preparedness for Y2K. As countries continue their remediation, testing and contingency planning, and as we get more information, some of our observations will change.

Y2K is a particularly challenging issue for analysis because of the uneven understanding around the world of the vulnerabilities of computer hardware and software, the unpredictability of failures among interconnected systems, and the wide variation in reporting and assessments of Y2K preparedness worldwide.

A quick tour around the world: Russia, Ukraine, China, and Indonesia are among the major countries most likely to experience significant Y2K-related failures. Many developing countries are having problems with a late start and with insufficient funds to carry out a strong remediation and testing effort. Countries in Western Europe are generally better prepared although we see the chance of some significant failures in countries such as Italy. Major economic powers such as Germany and Japan are making great strides in Y2K remediation, but even for them their late start and the magnitude of the effort suggests that even these countries are at risk of some failures.

Canada, the United Kingdom, Australia, Singapore, and Hong Kong are very well prepared and have a lower chance of experiencing Y2K failures.

While the United States probably will not be directly impacted by foreign Y2K failures, breakdowns in foreign infrastructure could impact our interests overseas. Disruptions and failures in telecommunication, electricity generation, and transmission and transportation pose the greatest threat because of their fundamental importance to all other critical services. Although a high priority for most countries, we estimate that only a few are on target in remediating and testing their telecommunications systems. Networks are likely to experience problems ranging from minor inconveniences to serious disruptions.

Experts are concerned that minor failures could cascade causing a network to become degraded over time. We are concerned about the safety of Soviet-designed nuclear plants due both to inherent design problems and to the lack of detailed data on Y2K remediation and contingency plans. Nonetheless, we judge that the chance of a nuclear accident on the scale of Chernobyl is extremely low. The chance of a lower level nuclear incident involving a Soviet-designed nuclear reactor is also low; but it is, however, higher than normal because of the fact that the power grid could experience failures, auxiliary generators could be inoperable due to maintenance problems or a lack of sufficient fuel, and erroneous data could lead to operator error.

Now we are highly confident that Y2K failures will not lead to the inadvertent or unauthorized launch of a ballistic missile by any country. We have been concerned about the potential for Russia to misinterpret early warning data because of Y2K-induced failures, especially if we were in a period of increased tension brought on by some international political crisis. However, Russia has agreed to cooperate with the United States on shared early warning data in order to prevent any misunderstandings resulting from Russian early warning failures.

Public behavior in response to Y2K-generated failures will vary widely. In developing countries, populations have minimal access to Y2K-vulnerable public services, and those who do are accustomed to frequent breakdowns. But countries with crowded, urban populations could experience significant unrest if outages are prolonged. The reactions of urban populations in developed countries are harder to gauge because of widespread media attention and high public awareness of the issue. We expect that the risks of panic are higher in countries with lower interest in Y2K.

We are, for example, concerned about possible Y2K-related interruptions in countries planning major tourist events such as Italy, Egypt, Brazil, and the Caribbean, should local infrastructures experience significant failures.

Y2K-related malfunctions have the potential to cause or exacerbate humanitarian crises through prolonged outages of power and heat, breakdowns in urban water supplies, food shortages, degraded medical services, and environmental disasters resulting from failures in safety controls. Russia, Ukraine, China, Eastern Europe, India, and Indonesia are especially vulnerable due to their poor Y2K preparations and, in some cases, the difficulty of coping with breakdowns in critical services in the middle of winter.

Few governments outside the West would be capable of managing widespread humanitarian needs. Although many have systems experienced in delivering medical and social services following natural disasters, Y2K failures present a more complex challenge because of the potential for multiple and simultaneous disasters within specific countries and around the world taxing the ability of international organizations to help.

Y2K failures in necessary communications system and in needed medical and social service would compound difficulties in mobilizing emergency responses. We have seen, in different months, an increasing number of statements by countries and commercial enterprises that they are now prepared for Y2K. We expect to see more such claims as the end of the year approaches. While progress has certainly been made on many fronts, not all of these readiness claims are credible, and it is a challenge for us to sort out the truth. Some governments and commercial enterprises have an incentive to overstate the Y2K problem while others are likely to downplay the risks of Y2K failures.

We are continuing to focus heavily on this evolving issue to ensure that our policymakers are as prepared as possible for the potential consequences for the United States and our allies of international Y2K failures. Thank you, Mr. Chairman.

Chairman GILMAN. Thank you Mr. Gershwin.

[The prepared statement of Mr. Gershwin appears in the appendix.]

Chairman GILMAN. Our panelists have certainly given us some food for thought. Let me start the questioning, and this is directed to our State Department representative, Mr. O'Keefe. GAO has reported that it has not seen well-documented and thoroughly tested Y2K emergency plans in place for overseas embassies, consulates, and missions.

Mr. O'Keefe, what assurance does the Department of State have that these posts can continue to perform key operation during the rollover, including providing services and information to Americans who live outside of our embassy confines?

Mr. O'KEEFE. Mr. Chairman, as I mentioned in my testimony, we have based the preparations for Y2K on existing procedures. As you well know, our embassies, throughout the years, have experienced earthquakes, civil disturbance, bombings, civil war, and we manage crises on a regular basis. In any particular year, we have 20 to 30 task forces for whatever emergencies that occur. So it is something that we do regularly.

But just to provide you the kinds of assurances which I think you and the American public deserve, I would note, first of all, that we have done crisis management exercises with Y2K, as part of that, at over 90 embassies already this year to make sure that they have their emergency plans ready and take into account Y2K problems.

Beyond that, as I had also mentioned, because GAO had pointed out that we had not well-documented the contingency plans and how they were going to function, we have instituted this validation process which embassies have to provide to us by the end of this month. Then by November 11th, we will have reviewed and provided comments back.

Chairman GILMAN. Thank you, Mr. O'Keefe. Has the Department distributed any extra resources to help the posts prepare for any possible Y2K failures?

Mr. O'KEEFE. Yes, sir, we have provided approximately $6 million for generators. We will also be providing another million for fuel. So that will allow all the posts abroad to operate for a minimum of 15 days should the local power grid fail. That will in turn allow us to communicate, will allow us to provide those essential services to U.S. citizens and continue the command and control function.

Chairman GILMAN. Thank you. Mr. Nygard, with regard to USAID, according to the 10th quarterly report that was issued mid-September of this year, six of AID's seven mission-critical systems are Y2K compliant. When will the New Management System be remediated, tested independently, validated, and certified as Y2K compliant? Are there any contingency plans for NMS if it is not Y2K compliant by the turn of the century?

Mr. NYGARD. Mr. Chairman, as I indicated in my testimony, we are in the very final stages of testing the NMS, and we expect it will be fully implemented by the end of this month—that is to say within another week and a half. We do not anticipate the need for contingencies, but the financial contingency plans that we have and that I described in some detail would cover the NMS as well as our other management systems should there be a failure. So we do not anticipate a problem and expect to have NMS fixed by the end of this month.

Chairman GILMAN. Thank you, Mr. Nygard. Mr. Gershwin, any special arrangements with your station chiefs overseas to make certain that communications won't be disrupted?

Mr. GERSHWIN. Obviously I cannot talk about all of that in an open session; but, yes, our own presence overseas is being worked very carefully for Y2K. We are thoroughly involved with helping with the embassy preparations themselves.

Chairman GILMAN. Thank you. Mr. Nygard, one more question. Why does only one mission in AID, Cairo, have a Y2K contingency plan? What assurances does AID have that its overseas missions are ready for Y2K and can continue to perform any critical assistance operations?

Mr. NYGARD. Mr. Chairman, while Cairo is the only mission that has a formally documented contingency plan, we do have contingency plans in all of our overseas operations. The levels of these have varied based on the size and complexity of the programs. As you know Egypt is our largest mission and our largest program. We have also done very detailed contingency plans in most of Eastern Europe and the former Soviet Union. For our other missions in Africa, Asia, and Latin America, similar kinds of contingency plans have been done, but not documented and not done in the detail that Cairo has been done.

Chairman GILMAN. Thank you, Mr. Nygard. Mr. Hastings.

Mr. HASTINGS. Thank you, Mr. Chairman. In a country like Pakistan that is recently in turmoil, has nuclear facilities, and we have, at least up to a certain point, had interaction with them, what, if anything, are we able to do or are we doing, taking into consideration that kind of government that is in a state of flux?

Mr. O'KEEFE. Mr. Hastings, we do obviously continue to have diplomatic relations with Pakistan; we do have our Ambassador there. One of our goals is stability. We do have certain legal restrictions because of the nuclear testing that both Pakistan and India conducted, so we cannot provide direct assistance to those governments. However, we can, through diplomatic means, continue the dialogue on the issue of safety and security of those weapons that they do have.

Mr. HASTINGS. Let me ask you two quick questions. What are the United States Government's greatest concerns for American citizens, both tourists and those living abroad? How successful have you been in convincing foreign governments of the seriousness of the Y2K problem? How closely have they worked with us, and which countries have done best and which have been the least responsive?

Mr. O'KEEFE. Sir, I would say that when you take a look across the spectrum of potential problems that, first of all, electric power grids tend to be a little more sensitive; and if you are in a cold country, that presents a little more problem. But for U.S. citizens abroad, probably the most difficult sector to get into and to fix is the medical sector. Because of that, we have instructed our embassies to consult doctors, hospitals, ambulance services, and local authorities regarding their contingency plans. We have an outreach strategy to the American public to tell them that if you have a medical condition, especially if you rely on electrical medical devices, you should be very careful about where you are going to travel.

With regard to heightening awareness of other countries, as I said at the beginning, it certainly is not a lone wolf effort. We have worked with the President's Council in Year 2000, with the U.N. through the G8, through APEC, through OAS, all of these international organizations to heighten awareness. It really has been quite a difference from the time I started on this about this time last year to right now. There is not only more awareness but there has been a lot more remediation and certainly a lot more contingency planning. In terms of worst and best, I wouldn't want to characterize one way or another.

Mr. HASTINGS. Mr. Gershwin, regarding nuclear power plants, even if Y2K does not cause them to fail and pose a danger, some of us are concerned about the synergistic effect of Y2K disruptions to emergency response infrastructures that would have to deal with a nuclear plant accident. Many states that have the old Soviet-designed reactors don't have the best safety culture or emergency plans in the best of times. Is there a risk? If there is a problem with a plant, that problem could become magnified by Y2K disruptions of emergency responders. Do countries like Ukraine have enough backup generators and fuel necessary for the remediation that I keep hearing about.

Mr. GERSHWIN. The issue that you raise is clearly the issue of the day for that part of the Y2K problem. We, both the U.S. Government and international bodies, have been very active in the former Soviet Union and in a variety of countries, working with the operators of nuclear reactors on surveying their Y2K preparedness, surveying the adequacy of their backup, the adequacy of fuel and so on.

The issue has gotten a great deal of attention this year, and there has been a very good response, in fact, from both the Russians and some of the other countries that have these reactors. The Department of Energy has been active, as well as the International Atomic Energy Agency. A great deal of attention is being paid to it. The problem is that these are necessarily very complex facilities that they operate in order to provide power. So, yes, as I indicated in my statement, there is concern about this. We don't think the chances are very high that anything very serious will take place. But there is somewhat greater risk just because of the interaction with the Y2K problem, particularly if power goes off and they have to start dealing with contingencies for which there hasn't been enough time to prepare.

Mr. HASTINGS. One very brief question, and maybe some of you can give me a followup and not bother to respond right now; but when the rollover occurs, some of us are wondering when do we consider that there will be quietus? Assuming everything goes well all over the world, when will it stop? I will get that answer from you subsequently.

My bigger question for government is, have we prioritized in a coordinated manner specific areas of specific countries that, if they went down, would adversely affect United States interests? Toward that end, Mr. O'Keefe, I heard you mention task forces. Are they being regionalized such that they are positioned to move where the problem may exist, and are there plans to anticipate where the greatest problems might exist?

Mr. O'KEEFE. Mr. Hastings, we have done this process of identifying countries where there was a fairly high potential for failure and also U.S. interests which could be affected by those failures, and this has been a process which has been ongoing since February.

Yes, we have. I can, in broad terms, say that areas where we do have U.S. forces stationed are obviously very key to our national interest and our security. Areas where we have a lot of U.S. citizens residing, they also are places where we are very concerned.

With regard to task forces, we have a rollover task force; and in that task force, we have regional representatives from each area of the world. In addition, we have the functional groups political, military bureau, the consular affairs bureau, and some that usually don't join in, like our financial management and planning to make sure that we can keep functioning in terms of payment and that sort of thing.

The way it would work would be if, in fact, we have a crisis point. Let's say our reporting would start at 7 a.m., December 31st from Fuji and New Zealand. As it rolls through, if we see a crisis point at that time, we will have the regional representative, and we would bring in more people. We would also coordinate very closely with the Department of Defense. Because, as this issue develops, I think that we are going to have a problem of resources. We would want to make sure that we rope everyone in, FEMA, Defense, domestic agencies.

Mr. HASTINGS. Thank you, Mr. Chairman. I am going to go vote.

Chairman GILMAN. Thank you, Judge Hastings. We will probably try to continue. We have asked one of our Members to go over now and we will continue with our hearing. I want to thank our panelists for being here with us this morning and giving us important information with regard to our preparations for the Y2K. The panel is dismissed, and we thank you again for your patience.

We will now proceed to panel No. 2. The second panel, as I indicated earlier, consists of Ms. Jacquelyn Williams-Bridgers, Inspector General, Department of State; Theodore Alves, Assistant Inspector General for Audits for U.S. Agency for International Development; and Ms. Linda Koontz, Associate Director, Accounting and Information Management Division of the United States General Accounting Office.

If our panelists would be kind enough to take their places at the witness table, we will proceed. I welcome our panelists and again remind them that they may put their full statement in the record and summarize as they deem appropriate.

I will have to temporarily put the panel in recess until Mr. Burr returns; he is on his way back, so if you would just stand by, thank you.

[Recess.]

Mr. BURR. [presiding] The hearing will come back to order. At this time I think we have called up the second panel, and I apologize for votes and hopefully that will be the last interruption that we will have. I am sorry that I did not have an opportunity to ask questions of the first panel, so I will try to use those that were appropriate and maybe ask the second panel double questions. Let me at this time welcome the Honorable Jacquelyn Williams-Bridgers, Inspector General, United States Department of State; Mr. Theodore Alves, Director Assistant Inspector General for Audits United States Agency for International Development; Ms. Linda Koontz, Associate Director Accounting and Information Management Division United States General Accounting Office.

Mr. BURR. Welcome to all three of you. We will start with Ms. Williams-Bridgers. You are recognized for an opening statement.

Ms. WILLIAMS-BRIDGERS. Thank you very much, Mr. Burr, for the opportunity to testify before this Committee on the results of our most recent analysis of global Y2K preparedness. My statement will address the OIG's oversight of Y2K remediation efforts by countries that host our embassies and consulates and by the U.S. Department of State.

With the permission of the Chair, I will provide a summary of my statement and request that the full statement be made a part of the record.

Mr. Burr. All full statements will be.

STATEMENT OF THE HONORABLE JACQUELYN L. WILLIAMS-BRIDGERS, INSPECTOR GENERAL, UNITED STATES DEPARTMENT OF STATE AND THE BROADCASTING BROAD OF GOVERNORS

Ms. WILLIAMS-BRIDGERS. Thank you. Over the past year, our work has revealed some key themes. Industrialized countries are well ahead of the developing world in their readiness to meet the Y2K challenge. Developing countries are generally lagging behind and are struggling to find the financial and technical resources needed to solve their Y2K problems, especially in the telecommunications, transportation, and energy sectors. Key sectors in the Newly Independent States and other former Eastern bloc nations are a concern because of the relatively high probability of Y2K related failures. Our assessments have suggested that the global community will likely experience varying degrees of Y2K-related failures in key sectors such as energy, telecommunications, and transportation in every region and at every economic level.

We are also assisting the Department in certification of its mission-critical systems's compliance with Y2K requirements by ensuring that every feasible step has been taken to prevent Y2K failures. We will review the adequacy of documentation for all mission-critical systems' certification packages which, by agreement with Under Secretary for Management Bonnie Cohen, must pass through OIG before submission for Y2K certification. OIG has evaluated one half of the 54 mission-critical certification packages prepared to date.

In this statement, I will discuss the results of recent OIG visits to a number of countries to assess their Y2K readiness, the need to better inform the public about host country readiness and potential disruptions of services and, last, the need for a post-Y2K assessment in order to identify lessons learned and best practices that may be applicable to government agencies and private sector organizations.

Over the past year and a half, my office has actively engaged with our embassies and host country government and industry representatives to establish venues for information sharing and cooperation. To give you a sense of our visits over the past 2 months: In Saudi Arabia, we found that the Saudi petroleum sector began its Y2K efforts in 1994 and has since completed remediation, testing and certification of its systems. Saudi Arabia has one of the most advanced telecommunications systems in the world and will reportedly be 100 percent compliant by the end of this month.

In Egypt, our government is strongly supporting the Egyptian government's Y2K Program. This effort includes nearly $16 million in U.S. assistance targeting, among others the power, telecommunications, health, water, wastewater, and civil aviation sectors. The Suez Canal Authority says that it will keep the canal clear of ships from around 11 p.m. on December 31st through the early morning hours of January 1st. During this transition period, canal pilots will inspect shipboard navigation and other systems of transiting vessels.

In Nigeria, infrastructure is not heavily dependent on computers and thus is not at a high risk of failure due to Y2K. Much of the emphasis on Y2K remediation in Nigeria has centered on the banking and petroleum sectors. The latter appears to be the best prepared.

In South Africa, we learned that their efforts have focused on six potentially high risk areas including electricity, water, communications, and health services. The biggest problem is that Y2K-related disruptions in other African countries might result in an influx of refugees similar to that which occurs when there is political instability in the region. But the government is prepared to deal and monitor with such developments.

While in South America we visited Brazil, which has made good progress in the Y2K Program in the areas of banking and finance, electricity, and communications. There is less certainty about the

Y2K readiness in two key areas: Water sewage, wastewater treatment is one; the second, small- and medium-sized businesses. Although these businesses are suffering the effects of an economic recession in Brazil they remain a critical link in its trade network and account for approximately 70 percent of the nation's economy. Yet small- and medium-sized businesses have generally gotten off to a very late start in their Y2K efforts.

A critical step in fully addressing the Y2K challenge over the next several weeks will be to get what we know about country readiness into the hands of U.S. citizens. The Department's recently issued consular information sheets serve as a useful tool to provide critical information to U.S. citizens. However, based on a review of sample information sheets my office has concerns about their adequacy. Some of the information sheets are too vague, contain too much boilerplate language, and do not fully capture the scope and content of the Y2K information collected by our overseas posts.

We recognize that in many countries information concerning the level of Y2K readiness is sensitive given the potential impact that Y2K might have on the country's economy, its reputation, and even its internal political stability. Nonetheless, so that Americans can make informed decisions about where they plan to be on December 31st, we recommend that the Department release additional information on country readiness as it becomes available.

Before closing, I would like to turn to the matter of what happens after Y2K, assuming the worst case scenarios do not come to pass. By January 1st, organizations around the world will have spent hundreds of billions of dollars to resolve the Y2K problem. Given this cost and the disruption that Y2K has produced over the past 2 years, we have to ask ourselves what have we gained from this investment besides the ability to continue operations as usual? The other question is how can we avoid the next Y2K-like technology glitch?

I would suggest that we have much to learn from the Y2K experience. Indeed, the collective efforts of both public and private sector organizations worldwide to resolve the Y2K problem may provide some important lessons, including best practices that may be applicable both to government and industry. My office is planning to address these issues over the coming year, and we would welcome any suggestions that the Committee might have to offer.

In conclusion, between now and the end of the year, the Department faces a difficult challenge of maintaining the momentum that it has developed and keeping the world focused on the Y2K problem. While much progress has been made by a large part of the international community to prepare for Y2K and to develop contingency plans, much of this effort will be for naught if complacency is allowed to take hold. The Department has a clear role to play over the next 2 months through its efforts to continue to fine tune its own contingency plans, to collect information on host country Y2K readiness, and to assure the American public is adequately informed about global Y2K readiness.

That concludes my summary statement, and I will await questions at the appropriate time.

[The prepared statement of Ms. Williams-Bridgers appears in the appendix.]

Mr. BURR. The Chair will recognize Mr. Alves.

STATEMENT OF THEODORE ALVES, DIRECTOR, ASSISTANT INSPECTOR GENERAL FOR AUDITS, U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT

Mr. ALVES. Thank you, Mr. Burr, for the opportunity to testify before this community about our oversight of USAID's efforts to address Year 2000 challenges. As you suggested, I will summarize my prepared testimony highlighting the most significant issues.

My testimony today focuses on USAID management efforts to prepare business continuity and contingency plans. To summarize, our audits have found that after a slow start, USAID has made significant progress to mitigate the risks posed by Y2K. However, our work also shows that USAID has not prepared contingency plans for some important development activities. As a result, it faces increased risks that it could encounter disruptions that would limit its ability to continue providing humanitarian aid and development assistance. This situation exists primarily because USAID has not clearly assigned responsibility and authority for developing contingency plans.

Before I describe our audit results, I would like to highlight some important USAID efforts to address the international implications of Y2K. These include developing contingency plans for its financial management operations, conducting detailed assessments of about 50 USAID missions, and creating tools to help developing countries address Y2K challenges.

Regarding prior OIG audit results, we have issued several reports and other products that have helped USAID management focus its attention to Y2K issues. In July 1997, we reported that USAID had not implemented GAO's suggested practices for addressing Y2K issues. In addition to implementing several specific recommendations, USAID committed, at that time, to follow GAO's guidance in its Y2K efforts.

In September 1998, we reported that USAID had strengthened its program but that it had not completed some important assessment phase activities. We recommended that the Administrator clearly assign responsibility to implement an effective program and that the responsible official direct USAID bureaus and missions to develop and test contingency plans. USAID agreed to implement our recommendations, but has yet fully done so. As a result the actions taken did not fully correct the problems.

We also devoted resources to ensure that USAID considered the impact of Y2K problems could have on developing countries.

Regarding contingency planning, our current work shows that USAID faces increased risks of encountering disruptions to its development assistance programs because bureaus and missions have not completed contingency plans. We found that USAID did not follow GAO's guidance for three of the four business areas we reviewed. Only the Office of Financial Management had prepared a contingency plan.

My prepared testimony includes three examples of bureaus and offices that are at risk because they have not prepared contingency plans. Responsible officials were relying on an expectation that existing procedures would be adequate. One official told us that he did not think Y2K would create significant problems. Given the risks involved and USAID's prior commitment to complete plans, these responses were disappointing.

The problem occurred primarily because USAID has not clarified responsibility to ensure that contingency plans are completed as we had previously recommended. According to a senior USAID official, the Administrator met with the head of each bureau to emphasize the importance of completing contingency plans and subsequently received assurance that the bureaus had adequate plans in place. Although this action partially addressed the recommendations, it did not correct the problem because USAID did not identify a single manager to be responsible and held accountable for ensuring that plans were completed.

Because little time remains to prepare for Y2K disruptions, we believe USAID needs to focus now on completing contingency plans. Specifically, USAID needs to make a senior executive responsible and accountable and require bureaus and missions to prepare contingency plans for their development assistance program functions.

In conclusion, Mr. Chairman, USAID has made significant progress addressing the Y2K challenge but needs to now focus its attention to developing business continuity and contingency plans in order to ensure that its important humanitarian and development assistance activities will not be disrupted.

This concludes my remarks, and I will be pleased to answer any questions you or other Members of the Committee may have.

Mr. BURR. Mr. Alves, thank you for your testimony.

[The prepared statement of Mr. Alves appears in the appendix.]

Mr. BURR. I am going to quickly go back and reread some testimony from the group before this. Is Mr. Nygard still in the room? I will assure you, from some of the things that I heard you say, he is going to have another opportunity to come back up here.

The Chair recognizes Ms. Koontz.

STATEMENT OF LINDA D. KOONTZ, ASSOCIATE DIRECTOR, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Ms. KOONTZ. Thank you, Mr. Burr, I appreciate the opportunity to participate in today's hearing on State and USAID's efforts to address the Year 2000 technology problem. I would like to summarize my statement briefly.

We have already heard from both State and USAID on the positive steps they have taken to increase worldwide awareness of the Y2K problem, assess international preparedness, and inform American citizens of Year 2000 related risks. Further, you have heard of USAID's efforts to mitigate Year 2000 risks associated with USAID-funded development projects.

Based on our review, we believe that State and USAID generally have reasonable strategies in place to deal with these issues. However, they have been much less effective in the area of business continuity and contingency planning, and I would like to spend the balance of my time focusing on this issue.

Despite extensive remediation and testing of mission-critical systems by State and USAID, there is a very real possibility that problems may occur in the millions of lines of code that were fixed or in overlooked embedded chips or commercial products. In addition, outside systems that exchange data with these agencies or infrastructure services like power or telecommunication may fail. These risks, coupled with the risk of Year 2000-related failures in foreign countries, mandate that these agencies develop comprehensive business continuity and contingency plans to ensure that core business processes can be continued both domestically and internationally. GAO has developed guidance on this topic, and OMB has adopted it as the standard to follow.

As required by OMB, State developed an enterprise-wide business continuity and contingency plan in June, 1999. However, we found that State's plan does not follow the mission-based approach which we recommend. For example, the plan does not identify State's core business processes or the minimum acceptable level of service for these processes during an emergency, and it does not identify the impact of the failure of mission-critical systems on core business processes.

In addition, the plan didn't indicate when or how State will test and evaluate its plan. As such, we do not believe this plan provides adequate assurance that the department is prepared to continue critical business functions in the face of Year 2000 failures. State officials told us that they plan to complete Department-wide contingency plan testing around mid-November, 1999. In addition, according to State officials, they will be issuing a revised plan next week which they believe will meet all the OMB requirements. However, we have not yet had a chance to review this revised plan.

Also, because of the varying conditions around the world, State also required that each embassy and consulate develop a business continuity and contingency plan. To assist, State developed a Y2K contingency plans tool kit in early 1999. The tool kit provided an appropriate and detailed methodology for identifying critical business processes, assessing Year 2000 related risks, linking the many existing emergency procedures the embassies already to have to Year 2000 failure scenarios, and identifying any additional resources that would be needed.

We reviewed the tool kit submissions prepared by ten embassies located in countries that were of particular interest to this Committee and found that all were incomplete. Although most of the submissions identified critical business processes as well as additional required resources, only two linked existing contingency procedures to Y2K failures or identified any additional procedures that would be needed. Further, there was no evidence that any of the plans had been tested.

Without the kind of thorough analysis called for in State's tool kit, there is no assurance that embassies and consulates are fully prepared for Y2K failures. State officials, however, have been responsive to our concerns and have developed a web-based tool that will be used to review and evaluate contingency plans at each post. They expect this validation to be completed by November 11th.

Let me briefly turn to USAID. You have already heard from a representative of USAID's Office of Inspector General, who gave a detailed assessment of the agency's Y2K business continuity and contingency planning efforts. We also reviewed USAID's enterprise-wide business continuity and contingency plan dated June, 1999. We found that USAID's plan is incomplete and found little evidence that the GAO methodology was followed. Furthermore, only one mission, Cairo, has prepared a Year 2000 contingency plan for its specific location. USAID officials stated that despite the absence of documented plans, some business continuity and contingency planning activity has been under way. However, they could not validate the extent to which the planning activity had actually occurred.

Given the results of our and the IG's work, we are very concerned about USAID's ability to sustain its core business functions during the rollover and protect its overseas personnel from Year 2000-related failures.

In conclusion, in the remaining days ahead, State and USAID will need to marshal their resources, strengthen their business continuity and contingency plan to help mitigate Year 2000 related failures and work toward maximizing assurance that they can perform their core business functions and maintain their overseas business operations during the rollover.

This concludes my remarks, and I am happy to answer any questions that you might have.

[The prepared statement of Ms. Koontz appears in the appendix.]

Mr. BURR. Thank you, Ms. Koontz. Thank you to all of our witnesses. I am going to turn the clock off, since it is just the Chairman and me. I think he has to take a phone call.

Let me start with you, Ms. Koontz. Is it safe to say that any agency that is focused on compliance as a new aspect of what they are doing should realize that it is too late and that that effort could best be spent on contingency?

Ms. KOONTZ. Are you talking specifically about the State Department or just in general?

Mr. BURR. I am talking about in any area where they have not identified a problem or are currently working on a solution to a problem, is it not too late? Don't we need to be more concerned with the contingency?

Ms. KOONTZ. Absolutely at this late date, we are about 2 months away from the Year 2000. At this point, the best bet is to concentrate even more greatly on contingency planning.

Mr. BURR. In your estimation as it relates to State, how far do we have to go before we can have contingency plans for all areas that we should?

Ms. KOONTZ. Although we found some deficiency in both the enterprise-wide and embassy plans, I think that if the State Department follows through with what they have told us that they were going to do, that is to validate the embassy plans and draft a new enterprise-wide plan, I believe that they will be able to complete these efforts in time.

Mr. BURR. Ms. Williams-Bridgers, if I understood you correctly, you said that the Inspector General's Office has had an opportunity to review one half of the mission-critical package.

Ms. WILLIAMS-BRIDGERS. That is correct.

Mr. BURR. What is the timeframe for the second half?

Ms. WILLIAMS-BRIDGERS. We are hopeful that the Department will present the certification packages to us so that we can complete our review of those packages prior to the end of the year.

Mr. BURR. So the holdup is not on the part of the Inspector General looking at the packages; it is on the part of State's supplying the package?

Ms. WILLIAMS-BRIDGERS. We have reviewed all of the packages that have been submitted to us. We are currently reviewing one package right now and are awaiting the remainder of the certification packages from the Department.

Mr. BURR. With every day that ticks by, if your conclusion of that package is a flunking grade—insufficient, with every day that ticks by what are our options?

Ms. WILLIAMS-BRIDGERS. The grades that have been given to agencies in the past have been based on their implementation of certified Y2K compliant systems. The Department recently received an A grade from Congressman Horn because they have implemented 100 percent of their systems. They are considered to be Y2K compliant.

Mr. BURR. I think there is a big distinction there that I want to draw. There is a big distinction between compliant and contingency.

Ms. WILLIAMS-BRIDGERS. Correct, absolutely. There is a very big distinction.

Mr. BURR. I think the focus of his efforts and the efforts of that Committee has been are we doing the things that we have identified, and do we have a game plan as to how we fix them by a certain date. Now let me ask you relative to contingency.

Ms. WILLIAMS-BRIDGERS. OK.

Mr. BURR. Where is your comfort level relative to contingency plans that exist for the functions of State and all the different areas?

Ms. WILLIAMS-BRIDGERS. I would agree entirely with the GAO that contingency planning is very important at this late stage in the year. That is where our attention should be focused. We are quite hopeful that the Department will be able to prepare and complete all of its contingency plans and test those contingency plans within the next several weeks, and we will be continuing to monitor that.

Mr. BURR. I have looked back in my own files, because earlier this year I did not feel that anybody was dealing with contingency, so I met with every department and I asked for their contingency plans on March 2nd. I wrote the Speaker, the Minority Leader, Congressman Bliley, and Congressman Horn, a memo that was sort of my overview, having met with all of the different agencies as to where they were specifically with regard to contingency plans. Hearing what you both have shared with me about State and looking back at what I wrote based upon what I was told, one might read this and believe that it was a fictional piece, because I actually raved about what they told me they were going to accomplish as it related to contingency. I don't get the impression you are here raving today.

What do we need to do? What can Congress do, if anything, to make sure that we are prepared whether there is or is not a problem? It would concern me, Mr. Alves, if there is, I think you said, a responsible person who suggested there is not a problem and he is a key link to both compliance and contingency. I would hope that we could have some influence on at least his willingness to carry forth.

But what can we do?

Ms. WILLIAMS-BRIDGERS. I think the most important thing for the Congress is to continue to provide oversight over the efforts of the various agencies. The continued encouragement, the continued monitoring of agencies' attention to contingency planning. In the case of the State Department, continued monitoring of the types of information we get into the hands of U.S. citizens is most important, particularly when there is a balance that must be maintained between the sensitivity of giving out information to the public and the need for the public to have critical pieces of information in hand so that they can make informed decisions.

Mr. BURR. I would take it that State is no different than every other agency. There was a time line that was established for everyone to be required to turn in contingency plans and for those to be tested. Am I correct?

Ms. WILLIAMS-BRIDGERS. Yes, I believe that that is correct. That there was a time line for contingency planning as well.

Mr. BURR. You have reviewed 50 percent of the mission-critical issues. Have they already passed the time line that was set?

Ms. WILLIAMS-BRIDGERS. Actually we are right on schedule with our time line expected for review of those mission-critical systems.

Mr. BURR. Let me go to your example that you used on the Suez canal, that shipping would stop and they would take the responsibility to review the navigational equipment on each vessel to make sure that from a safety standpoint, I would take it that they felt comfortable 6 hours later when everything started to move.

Let me ask you as it relates to international waters; if they have that concern with the vessels that exist in the Suez canal, who is going to check the ones that are on the open water?

Ms. WILLIAMS-BRIDGERS. Actually, there has been much attention in the international community and among international professional associations governing maritime industry and the ports and canals, and there is a similar strategy being employed in many of the canals that they will not allow ships into the canals unless they have been given some prior assurance by the ship owners that they are Y2K compliant. They don't want to create bottlenecks in the canals. There will be onsite inspections of many of the vessels before they are allowed to enter to give that added assurance.

Mr. BURR. I also serve on the Commerce Committee, and one of the reasons I am a little preoccupied is that I have a Y2K hearing going on at the same time across the courtyard on medical devices. But one of the areas in which we have acknowledged concern is the flow of petroleum for that period, because we are concerned with the computer capabilities of a lot of the tankers—genuine concern, do you think?

Ms. WILLIAMS-BRIDGERS. Yes, I think there is a concern, and that is why the United States is looking particularly at those countries that provide a key link in our trade networks in the transportation of goods and services, including fuel, and the readiness of countries as well as the port authorities to handle that Y2K problem. So, yes, that is an area to which we would pay particularly close attention.

Mr. BURR. Given that you have reviewed a lot of the mission-critical things for State and, I think, understand their contingency efforts, let me ask as it relates to international finance. There are trillions of dollars that are transferred on a daily basis in the international markets. How involved, if any, is State in the review of those systems and their compliant status, and is that an area that we should be concerned on?

Ms. WILLIAMS-BRIDGERS. The State Department is not directly involved, of course, in the banking networks. But in the course of the work that we have done in our meetings that we have held in-country with host country officials, we have also met with some representatives of the banking industry. We reviewed all open source materials that reflect on the readiness of the finance sector and generally the finance sector got a very early start. We have some assurances that they are fairly well prepared to deal with the Y2K problem.

Even in regions of the world, even in countries where other sectors are significantly lagging and are considered at medium or high-risk of failure, their finance sectors generally tend to reflect a relatively low-risk of failure.

Mr. BURR. How involved is State relative to its advice, its response to questions by U.S. companies that might have interests abroad relative to the Y2K compliance of the country in which they might have interest?

Ms. WILLIAMS-BRIDGERS. Again, in our meetings in 31 countries over the past year, we have met with representatives of the American business community in many countries and found that there has been a good dialogue not only between the American business community and U.S. embassies, but also other English-speaking embassies in the country. We have found, in fact, as some best practices where the U.S. Embassy has developed consortiums, if you will, with representatives of the business community meeting with embassy representatives, to have discussions about what actions need to be taken, what kind of collaboration could occur within the business community between the business community and the diplomatic community.

Mr. BURR. Is that exchange taking place in your mind?

Ms. WILLIAMS-BRIDGERS. Yes it has.

Mr. BURR. Let me read a statement to all of you and ask you to comment if you agree, disagree, or if you have any comment:

"Working with our colleagues at the Department of State with Federal agencies and with our partners in the United States and overseas, we have made major progress in working to assure that our people and our programs won't be adversely affected by Y2K".

That is comments by the USAID. Do you agree or disagree with that statement?

Mr. ALVES. The focus of our work on contingency planning was on USAID's ability to continue with its business functions, carrying out its development assistance. USAID has worked closely with the State Department both at headquarters and at missions overseas to ensure the safety of USAID's employees. They have been working on developing specific contingency plans. But the focus of those plans has been limited to safety of employees rather than ensuring that we can continue to conduct our business of providing sustainable development assistance.

Ms. WILLIAMS-BRIDGERS. Most of our attention also has been focused on the Department's contingency planning for its own systems and delivery of services to Americans, and we have quite honestly in our oversight efforts not looked at the linkages with the USAID Programs. I would not be in a position to comment on the statement.

Mr. BURR. Is it naive of me to believe that if there are concerns about the core functioning, which I think are concerns that you have raised, Mr. Alves.

Mr. ALVES. Yes, that is our concern.

Mr. BURR. How can the services from that be expected to operate without adversely—how can the programs not be affected if we have a fundamental problem at USAID? I mean, am I misstating your concerns that exist there?

Mr. ALVES. No, you are not misstating our concerns. We believe that USAID's development assistance objectives are placed at risk because USAID has not focused its contingency planning efforts on being able to continue to provide that development assistance.

Mr. BURR. This is the testimony of Mr. Nygard right before you, and he said that the programs won't be adversely affected by Y2K.

Mr. ALVES. We may disagree on the extent to which USAID's Programs will be affected. We have discussed the issue with USAID officials including Mr. Nygard, and other officials have made a commitment to strengthen their contingency planning to focus on development assistance efforts.

Mr. BURR. Ms. Koontz?

Ms. KOONTZ. I would like to add, we agree with what USAID's IG has done, and it is true that USAID has done a lot of work overseas to work with foreign governments to ensure that development projects that have been funded by USAID are Y2K compliant. However on the issue of USAID's ability to continue its business processes and provide critical services, it has not done enough planning in my view to assure us that they are going to be able to do that.

Mr. BURR. Have they done enough planning to say at this hearing that they won't be adversely affected by the Y2K?

Ms. KOONTZ. I would have to say no, based on what we have reviewed.

Mr. BURR. Do they know how the Y2K issue is going to affect them yet?

Ms. KOONTZ. I don't believe so. Part of the contingency planning process is to assess the risk to your programs. Until USAID goes through that process, I would have to say they would not know what the risks are to their programs at this point. So they need to go through the contingency planning process to arrive at that conclusion.

Mr. BURR. How having not identified it yet, it is pretty tough to make the claim that nothing would be adversely affected. The State Department has a tool kit. Does USAID have a tool kit? Do they have anything?

Mr. ALVES. AID is using the State Department tool kit.

Mr. BURR. They are using the same one?

Mr. ALVES. Yes they are. While we talk about focusing on business processes, USAID has done some work focusing on financial systems. I think what happened is that early in the contingency planning process, they ended up shortcutting the process of identifying their core business. Early in the process USAID managers have identified the ability to obligate money, award contracts, and make payments as their core business process. They then focused their attention on developing contingency plans for these processes without having looked at their development assistance activities, where they are actually providing the assistance. I think that is part of the flaw of what happened here. Responding to our audit findings, USAID managers have committed to pay special attention at this point to focusing on the development assistance activities.

Mr. BURR. Let me just ask Ms. Williams-Bridgers, any feedback from the overseas posts relative to the tool kit, and have there been any significant changes made to it over time?

Ms. WILLIAMS-BRIDGERS. With regard to the contingency plans, we are waiting to get some information back from the Department on this web-based tool that Mr. O'Keefe offered earlier today. We have not gotten feedback on the implementation of that tool kit. However, on our most recent visit to posts, we were anxious to see that contingency plans were being completed and tested at our posts; and they had not been as recently as the last couple of weeks.

Mr. BURR. I am sure this is not a surprise to any of our witnesses as I am reminded daily when I call home, Christmas is right around the corner. I guess it is just 60 days now or fairly close to it, as my wife likes to remind me as we miss targets of when we are going to adjourn up here. Sixty days is a very short time with a tremendous amount to accomplish. I would urge each of you that you remain as vigilant as possible. Where this Committee, where this Congress can help to increase the level of intensity to make sure that if there are problems, that we have a plan to address them and that, therefore, the services and the functions of that area are affected as minimally as they can be, that is the objective of what we are after. If, on January 1st later in the morning we all wake up and find that we don't have a problem, I think that there will be a lot that we have learned. There will be money that has been spent to further develop technology and, more importantly, the human mind.

Thomas Jefferson said, I am not an advocate of frequent changes in laws and constitutions, but laws and institutions must advance to keep pace with the progress of the human mind. This is really a process of our keeping pace with where the human mind has taken us, and I thank each of you for your willingness to testify.

Does the Chairman have questions?

Chairman GILMAN. Yes, thank you very much. Thank you, Mr. Burr, for taking over while I was detained.

Ms. Williams, according to GAO and OMB, the Department's Y2K business continuity and contingency plan is too high level to determine if risks have been fully addressed or are incomplete, and does not link State's core business processes to its contingency plans. What is the Department doing to better prepare and plan for the Y2K rollover?

Ms. WILLIAMS-BRIDGERS. Mr. Chairman, we would agree with GAO's assessment of the lateness and the incompleteness of the contingency planning effort by the Department of State. We are hopeful that within the next 3 to 4 weeks that the Department will complete its worldwide contingency planning efforts and will begin testing contingency plans—something that we have not yet seen evidence of yet here or abroad.

Chairman GILMAN. Are you satisfied that they are going to be able to meet the problems?

Ms. WILLIAMS-BRIDGERS. I am quite hopeful. Given the level of effort, given the very reasoned and strategic approach that the Department has taken to date to its Y2K efforts, I think the Department has realized extraordinary progress, given the formidable challenge that was before it in looking at Y2K remediation efforts at some 260 locations around the world.

So we are quite optimistic that the Department will be able to accomplish all that needs to be done in order to overcome the Y2K challenge.

Chairman GILMAN. Inspector General, the Department issued consular information sheets for 172 countries in September of this year which included information on Y2K risks, but that information was fairly general in comparison to other actions. What is State doing to provide more detailed information that would allow the reader to discern differences between the countries, in other words, one that is generally prepared for Y2K from one that is somewhat prepared?

Ms. WILLIAMS-BRIDGERS. We, too, were quite concerned about the vagueness of many of the consular information sheets that we saw. We just looked at samples, about 29 of the consular information sheets issued, because we had direct knowledge based on our own visits in countries in those locations.

We do understand that the Department does intend to reissue or issue more updated consular information sheets within the coming months, and that they intend to provide more information than they previously did if they have evidence that there will be potential disruptions in country. We are hoping that the Department will be much more specific in the kinds of advice and counsel that they would give to U.S. citizens about what precautions they might take, given potential failures of certain critical services that they would come to expect.

Chairman GILMAN. With regard to that, has the State Department issued any travel warnings yet? Does it plan to do so? If so, what countries are they thinking about?

Ms. WILLIAMS-BRIDGERS. They have not issued any travel warnings which would advise the traveling public to defer travel to any country. We would hope, however, given that certain countries will not be able to overcome potential failures of some of their key sectors, that the Department would issue such travel warnings for those countries.

Chairman GILMAN. Thank you. Mr. Alves, with regard to USAID, since completing its evaluations of overseas missions on Y2K preparedness and the status of USAID-funded development projects in foreign countries infrastructure vulnerabilities, what has USAID done to assure that the problems identified are going to be corrected in time?

Mr. ALVES. USAID has made a commitment to us that they will focus their attention to completing contingency plans that address development assistance. We believe that time is short.

USAID has developed, to help developing countries, actually, a tool kit that provides a shortcut method to develop contingency plans. The intent was to use this for developing countries, and we believe that they can use the same approach for themselves to be able to complete contingency plans as quickly as possible and, hopefully, in time to be effective.

Chairman GILMAN. The Committee is aware of the problems USAID has experienced during the development of the New Management System. Aside from Y2K, what is the status of NMS? When will the system be fully operational?

Mr. ALVES. We have had issued a number of reports on the New Management System, very critical reports, as you may recall. At this point, USAID has reached the conclusion that the New Management System needs to be replaced. It is still in operation. It is more stable than it was earlier so that there are fewer flaws, but it still needs to be replaced.

USAID is working aggressively to replace the New Management System with a suite of commercial off-the-shelf systems. At the end of September, 1999 USAID awarded the first contract for the core accounting system, a commercial off-the-shelf system.

Chairman GILMAN. So they are still using the old financial management system?

Mr. ALVES. Yes, they are still using the New Management System; and, in fact, they have had to repair it so that it would work in Y2K.

Chairman GILMAN. According to the GAO and your office, AID's enterprise-wide and mission-level business continuity and contingency planning process needs to be greatly improved. At this late stage, however, what can AID do to help assure that it is prepared for Y2K failures here and abroad?

Mr. ALVES. As I mentioned a little earlier, USAID has prepared a tool kit to help developing countries to do contingency planning, and we believe that it can use that tool kit to focus attention on priority development assistance functions and develop contingency plans.

Chairman GILMAN. Ms. Koontz, you have reviewed the State Department's consular information sheets which provide data on how prepared foreign countries are on Y2K. What is your view of the information presented in those sheets? Based on the data, can our citizenry make informed decisions about whether they should be traveling or remaining in certain countries?

Ms. KOONTZ. Just like State's IG, we reviewed a sample of the consular information sheets, and we also found them to be very general in nature. Certainly the information that is presented is not as specific as the information that is presented in other sections of the sheets that deal with things like crime and transportation.

Further, we thought it would be difficult for a reader to distinguish the relative risk among countries. For example, it may be difficult to make a distinction between a country that is characterized as "somewhat" prepared as opposed to "generally" prepared.

Our understanding in our discussions with State is that they have more detailed information now than when they originally issued the sheets, and that they plan to update their web site with this information to make it more specific. In addition, when other information comes in, they plan to continue that updating process.

Chairman GILMAN. I assume that you are all part of a working group; is that correct? For watching over Y2K? Are you all part of a working group? Interagency working group?

Ms. WILLIAMS-BRIDGERS. Our office is not, but the Department of State is part of an interagency working group. We have attended some of these working group—interagency working-group sessions, though, upon invitation of State Department but have not been active participants in the interagency discussions.

Chairman GILMAN. Will you be an active participant between now and the end of this year?

Ms. WILLIAMS-BRIDGERS. We have been actively engaged with our agency and have had much interaction and discussion about the results of the interagency working group sessions. We intend to continue to be actively involved with our agency's Y2K efforts.

Chairman GILMAN. I would hope that all of you would be part of that since there is so little time and so much to be done yet.

I address this to the entire panel. What do you see as the most important thing we should be doing to bring us up to date?

Ms. WILLIAMS-BRIDGERS. I would say in the international arena, we believe that at this point in time that most countries are seriously engaged in addressing the Y2K problem, and we take comfort in that. Given that so many countries got such a very late start and given that the amount of resources that are necessary to fully remediate their systems will not be available to them in the form of technical and financial resources, it is imperative that these countries begin to triage their efforts to move toward contingency planning and move toward testing.

Chairman GILMAN. What do you do to bring that about?

Ms. WILLIAMS-BRIDGERS. I think it is imperative that constant consultation between the U.S. Government and host country governments continue.

Chairman GILMAN. Who does that consultation?

Ms. WILLIAMS-BRIDGERS. The embassies have been engaged in those consultations with host country governments and through the G8 sessions and other international forums.

Chairman GILMAN. Are the embassies making that a high priority?

Ms. WILLIAMS-BRIDGERS. Yes, they are. They have a huge stake in this because they rely on host country government infrastructure to provide mission-critical services. There are two other areas that we need to be particularly concerned about. The second is probably the most pervasive problem of Y2K, but that which we know the very least about are the embedded devices, the embedded chips, and as Mr. Burr had alluded to in his other Committee arena, in the health-care sector. We know that embedded chips prevail in a lot of the equipment which is Y2K dependent.

We know that there are hundreds of millions of these embedded chips in power plants and nuclear reactors and telecommunications switches, and we know very little about the potential impact of those embedded devices on the failure or the continued operation of their systems.

Chairman GILMAN. Are we providing information to other countries with regard to warning them about these embedded chips?

Ms. WILLIAMS-BRIDGERS. Yes.

Chairman GILMAN. How do we do that?

Ms. WILLIAMS-BRIDGERS. We have shared information in a variety of different forums through some of the professional associations, the international maritime associations, the port authority, ICAO, the international civil aviation organization. There has been much discussion about that very problem.

Last, I think that we have to guard against complacency; many people now are quite tired of hearing about Y2K. We had the 9/9/99 worldwide test, and that seemed to be rather uneventful. But I think we need to keep our guard up, as you suggest, Mr. Chairman, with continued engagement on our part.

Chairman GILMAN. Mr. Alves, any recommendations as the highest priority issue we ought to be taking up.

Mr. ALVES. USAID obviously needs to focus on contingency planning, but USAID also has a role to play in helping developing countries deal with Y2K issues, and USAID has developed a tool kit that is designed to help developing countries both remediate their systems and deal with emergencies and contingencies.

Chairman GILMAN. Is that widely distributed?

Mr. ALVES. It has just completed being tested, and it is about to be distributed. It is probably too late to help in remediating systems but it should be a help in contingency planning if it can be distributed widely enough.

Chairman GILMAN. How long will it take to distribute it widely?

Mr. ALVES. I think that within a couple of weeks of getting it out.

Chairman GILMAN. So by November, we are giving some contingency information.

Mr. ALVES. I am sorry?

Chairman GILMAN. By November, you are providing some contingency information?

Mr. ALVES. Not exactly. What the tool kit will do is provide a way for developing countries and organizations in developing countries to prepare contingency plans. So it is a road map to help them to be able to do it as opposed to——

Chairman GILMAN. Is that enough time?

Mr. ALVES. They are very late, but contingency planning can continue up until you encounter an event. So while I would not say that it is going to solve the problem because it is not a silver bullet it does provide a contribution that should help.

Chairman GILMAN. Sixty days to go, apparently. That is pretty short. Ms. Koontz, do you have any suggestions?

Ms. KOONTZ. There are a couple of priority areas particularly for the State Department, and the first is for them to continue to make the travel information in the consular information sheets more specific and more useful to the traveling public.

In addition, State needs to follow through on its business continuity and contingency planning, particularly for its overseas offices. The State Department has a tremendous advantage because there is a lot of very good guidance both outside the State Department and that which they have developed themselves that is very good, and if implemented, it should put them in a good position. However up to this time, implementation and follow through has not been what it should have been.

Chairman GILMAN. Who does the oversight on the implementation?

Ms. KOONTZ. To be frank, in terms of the embassy plans, I believe there was very little oversight of their preparation in this area. The guidance was given out to the embassies, but I don't believe that there was sufficient review of the plans that were generated.

Chairman GILMAN. Is there now sufficient review?

Ms. KOONTZ. I believe that what the State Department has told us is that they have developed a validation tool. I do not have all the details about that at this point in time. But anything that they can do at this point to look more closely at those plans and encourage embassies to fully assess and plan for the Year 2000 is what they need to do.

Chairman GILMAN. Are they preparing to do that? Is someone working on that?

Ms. KOONTZ. They say that they are working on it.

Chairman GILMAN. Who is going to be——

Ms. KOONTZ. We will continue to followup, of course.

Chairman GILMAN. Will the Inspector General be following up?

Ms. WILLIAMS-BRIDGERS. Yes, we will, sir.

Chairman GILMAN. Thank you. Mr. Sherman.

Mr. SHERMAN. Thank you, Mr. Chairman. I am told that the State Department has a system by which Americans abroad who are in trouble can seek help. Their family can wire them funds, et cetera.

It occurred to me that this system and many other services provided by our embassies and consulates could be very important to persons in those countries that are not dealing with the Y2K problem effectively.

But then it occurred to me that the embassy is probably not open on January 1st. January 2nd is going to be a Sunday, and I know that we do not ask our government employees who are not engaged in public safety and a few other emergency circumstances to work on the first day of the year or to work on a Sunday. Will American embassies and consulates in countries that are expected to have Y2K problems be open and available to American tourists and other Americans abroad or will there simply be a sign that says come back to us 48 hours after Y2K has struck?

Ms. WILLIAMS-BRIDGERS. Mr. Sherman, if I might, our embassies will be available. They will be staffed with personnel who have been tasked with reporting back beginning 1 hour after midnight and every hour for the next 24 hours.

The list of assignments and who should be in the embassies has already gone out, and people have been told to cancel all leave plans for essential personnel so that American citizen services will be provided to any American in need.

Mr. SHERMAN. So this is not just a matter of reporting back to Washington how things are going, but enough people to deal with what may be the largest group of Americans ever to seek embassy or consulate help in the absence of a political tumult at the same time.

Ms. WILLIAMS-BRIDGERS. Absolutely.

Mr. SHERMAN. Good planning. I have no further questions.

Chairman GILMAN. Thank you, Mr. Sherman. Again I thank our panelists for providing us your expertise and information. I hope you are going to stay on top of all of this as we find that there is a great deal more to be done. So with our admonition to keep on top, we thank you again. There may be some questions that might be submitted by some of our Members, and we would request that you would respond to those. With that, the Committee stands adjourned.

[Whereupon, at 11:55 a.m., the Committee was adjourned.]

APPENDIX

OCTOBER 21, 1999

NEWS International Relations Committee

U.S. House of Representatives * Benjamin A. Gilman, Chairman * 2170 RHOB * Washington, D.C. 20515

DATE: *October 21, 1999* *FOR RELEASE: Immediate* 1099-28
CONTACT: *Lester Munson, Communications Director, 202-225-8097, Fax 202-225-2035*

GILMAN PANEL EXAMINES Y2K THREAT TO U.S. INTERESTS ABROAD

WASHINGTON (October 21) – U.S. Rep. Benjamin A. Gilman (20th-NY), Chairman of the House International Relations Committee, released the following statement today at a committee hearing on "Y2K: A Threat to U.S. Interests Abroad":

"Our Committee on International Relations has engaged in comprehensive oversight of a number of issues affecting the foreign interests of our nation and on the Administration's policies that identify and advance those interests. In so doing, we have a further fiduciary duty to make certain that the agencies charged with protecting and advancing those interests are themselves in the position to do so effectively.

"In meeting our oversight responsibility in that regard, I asked the General Accounting Office to do a study of the readiness of the Department of State and the Agency for International Development to meet any Y2K challenges when the year 2000 begins.

"GAO was specifically requested to study three things: the first was whether the State Department, through its leadership of the President's Year 2000 Council International Relations Working Group, has an adequate strategy in place to assess and address international year 2000 risks.

"Secondly, we wanted GAO to ascertain whether the State Department has an adequate strategy in place to ensure the safety of Americans overseas who may face risks from year 2000 failures.

"Lastly, we need to answer the question of whether our Agency for International Development has taken the necessary appropriate steps to address with foreign nations any year 2000 risks associated with information technology projects and systems that USAID has funded.

"We are here today to hear not only their report but, just as importantly, to ascertain, on the record, the administration's position and views as to its readiness for problems that may come its way because of the Y2K phenomena. The administration will now be on the record as to its readiness.

"It is important that we press for this status report and an accounting for any state of unreadiness by either State or USAID. We need to know, to fulfill our fiduciary duty to the American taxpayer, whether the generous resources and legislative direction we have provided these agencies has been spent prudently and wisely and with the desired effect of protecting American interests abroad."

Testifying at the hearing were: Mr. Richard C. Nygard, Chief Information Officer, U. S. Agency for International Development; Mr. John O'Keefe, Special Representative for the Year 2000, U.S. Department of State; Mr. Lawrence K. Gershwin, National Intelligence Officer for Science & Technology, Central Intelligence Agency; the Honorable Jacquelyn L. Williams-Bridgers, Inspector General, U.S. Department of State; Mr. Theodore Alves, Director, Assistant Inspector General for Audits, U. S. Agency for International Development; and Ms. Linda D. Koontz, Associate Director, Accounting and Information Management Division, U.S. General Accounting Office.

Testimony of
Richard C. Nygard
Chief Information Officer, and Deputy Assistant Administrator For Management
U. S. Agency For International Development

Before The House Committee On International Relations

Thursday, October 21, 1999
Washington, D.C.

I appreciate the opportunity to appear before you this morning to describe the response of the U.S. Agency for International Development (USAID) to potential Y2K disruptions that may affect our Agency's systems, our programs and the countries in which we operate.

USAID frequently focuses on crises others face, such as our Agency's support for Hurricane Mitch reconstruction and humanitarian response in Kosovo. On behalf of Administrator Anderson, I want to assure you that we understand the significance of resolving the Y2K problem, so that our Agency's programs and operations can continue as we face these risks along with the rest of the world.

The condition of information systems at USAID has been a point of ongoing interest, and I am pleased to report on our progress related to Y2K readiness and contingency planning. I will also address USAID's role externally as a partner in the overseas efforts of the US government on Y2K, as one source for Y2K related humanitarian assistance through our Office of Foreign Disaster Assistance (OFDA), and as the sponsor of an initiative, the Global Y2K Consortium.

The Agency has almost 7000 employees worldwide, of which 2,000 are at its headquarters in Washington, DC. USAID's field structure is made up of 79 overseas missions and donor/coordinator sites in Latin America, the Caribbean, Africa, Asia, the Near East as well as Europe and Eurasia.

USAID's Internal Systems

By way of background related to internal Y2K activities at USAID, the Agency has a total of seven mission critical systems, two of which have been replaced. Of the remaining five, four have been repaired and implemented. Validation and implementation of the fifth system, USAID's New Management System (NMS), are on schedule for completion at the end of this month.

USAID is continuing to test Y2K readiness as other systems of the Agency are modified for new functionality. The methodology used to repair and test mission critical and other systems was provided by its prime contractor according to demanding technical standards and includes management practices such as specialized techniques for detailed measurement of Y2K progress and comprehensive testing. USAID has been working with its Inspector General (IG) and its prime contractor to expand improved technical discipline throughout the Agency's information systems management. By all accounts including our IG the trends are positive, but need our continued attention as a team.

Business Continuity Planning

USAID business continuity planning is occurring in three forms: formal continuity planning for our critical internal business systems; program review to assure that ongoing USAID activities will be able to continue after the rollover on January 1, 2000 and external coordination with the Department of State's contingency planning at each overseas post.

1. Internal agency Y2K business continuity planning for its mission critical systems focuses on three critical functions: payments, obligations and funds control. The internal business continuity and contingency planning program, in conjunction with technical assistance from a highly capable commercial firm, addresses the ability to handle, at an essential and minimal acceptable level, these three critical functions through any Y2K difficulty.

Y2K contingency plans began last fall with an analysis of financial processes followed by a ranking of the importance of each process and activity. This initiative included a series of workshops to review the core processes by which the three critical functions are accomplished. The business processes were broken into individual steps, and the risks of each failing at Y2K was examined.

USAID's Phase One internal "high-level" contingency plan was finalized in December 1998. Phase Two formalized detailed "work-around" techniques for the various business processes/activities identified in Phase One. Manual procedures and local spreadsheet applications were developed to facilitate interim operations if disruption to normal mission or Agency operations occurred.

As of October 15, 1999, all forty-four overseas missions that perform accounting functions for USAID have reported that their rehearsals of Y2K contingency plans for core financial functions have been completed and reported to headquarters as successful by the mission controllers. All forty-four Missions reported no notable start-up errors when FY 2000 operations were commenced in early October.

In addition, all of these forty-four overseas missions have reported that their testing of their electronic payment system has been successful, without any exceptions noted. This testing proved successful for the FY 1999 to FY 2000 transition in early October 1999. The test assured that the payment system link between overseas Missions and the U.S. Treasury used to make U.S. dollar payments was fully operational. Documentation of those rehearsals is in progress.

2. While USAID lacks the resources to assure that each of the countries within which we operate will not be affected by Y2K disruptions, we have undertaken significant actions to assure that our ongoing programs will continue after January 1, 2000. For each of our regional bureaus, 5 per cent of its FY 1999 development assistance budget was set aside to be used, as necessary, for Y2K program repairs. Before the funds could be used for purposes other than Y2K, the Bureau Assistant Administrator had to affirm that all prudent steps had been taken to make programs Y2K compliant. The USAID Administrator met with the bureau Assistant Administrators in early spring of this year, and a second series of meetings was held with the Acting Administrator during the summer to discuss Y2K compliance and the continuity of mission and program operations. The heads of all bureaus indicated that necessary steps had been taken by the end of FY 1999 to assure continuity of program operations. In addition, a number of actions were taken centrally to assist missions and programs in assuring program continuity. These included:

- Performing independent Y2K assessments on critical infrastructure and government systems, in coordination with host country missions and national Y2K Committees, in 50 countries. Y2K issues and problems discovered were reported to appropriate organizations (national, international or donor) for evaluation and planning. In select instances specific remediation support was provided in concert with on-going bilateral assistance projects.

- Training program and host country managers on industry-standard Y2K methodologies for assessment, inventory, remediation, testing and contingency planning.

- Making available contingency planning consulting and workshops for embassies, missions, program-funded activities and the host country.

- Cooperating with other donors (World Bank, European Bank for Reconstruction and Development, etc.) to develop programs to solve specific sector Y2K problems.

- Participating in Inter-government and international groups addressing the Y2K problem and support requirements. USAID's collection and reporting of host country Y2K status contributed to initiation of corrective support by other organizations.

- Developing the Y2K Management Tool Kit to help system-owners, government planners, business owners and community readiness leaders in the developing world, Eastern Europe and Eurasia tackle their Y2K challenges. The Tool Kits assist in the three vital, related areas of Y2K work: remediation, contingency planning, and community readiness. We encouraged the creation of the Global Y2K Consortium, which was incorporated in August 1999, to distribute the Tool Kits with the help of a growing network of Private Voluntary Organizations (PVOs). So far, more than 40 PVOs are participating in the distribution of Tool Kits.

3. Externally, USAID is working with the Department of State Y2K Committee under the authority of the chief of mission at each overseas post. Embassy Y2K Committees with participation of USAID mission staff continuously evaluate the host nation Y2K readiness and report their findings through the ambassador to Washington for the benefit of the larger foreign affairs community and the public. To provide additional support of mission, program and host country Y2K issues, USAID has established Y2K Resource Centers in Washington, Russia, Ukraine, and Egypt.

Humanitarian Assistance after January 1, 2000

Finally, if the consequences of Y2K requires humanitarian assistance internationally through our Office of Foreign Disaster Assistance (OFDA), USAID has taken these actions to prepare for the worst, while we hope for the best:

1. A worldwide guidance cable was issued earlier this year regarding Y2K and the possible responses for international disaster assistance that may be required. The guidance cable explains that the criteria for intervention will be initiated in response to an ambassador's declaration (or its equivalent).

2. USAID Communication systems were upgraded and improved to ensure Y2K compliance and ability to operate during the rollover.

3. Humanitarian assistance partners were encouraged, (UN Agencies and U.S. based PVOs) to be Y2K compliant and prepared to deal with possible consequences of Y2K problems.

4. The Agency's Humanitarian Assistance Operations Center (with potential expansion of additional capacity one off-site) will function 24 hour per day by 7 days a week if necessary during the critical period of January 1-15, 2000.

5. Strategically located stockpiles of food, blankets and emergency supplies are at capacity level.

6. OFDA has worked closely with the Department of State on its system of Y2K related embassy "weathervane reporting" to support up to date analysis of Millennium consequences.

We at USAID are concerned that the world's humanitarian capacity is currently stretched in Kosovo, Central America and in the African ongoing humanitarian crises.

The uncertain impact of Y2K could place major additional demands on our Agency and on other donors of humanitarian aid.

In closing, Mr. Chairman, let me repeat that we at USAID, working with our colleagues at the Department of State, with other federal agencies and with our partners in the United States and overseas, have made major progress in working to assure that our people and our programs won't be adversely affected by Y2K. I cannot guarantee that there will be no disruptions because of conditions in the countries where USAID operates, but I believe that the actions we and others have taken will ensure the safety of our people and the continuity of our programs.

STATEMENT OF JOHN O'KEEFE
SPECIAL REPRESENTATIVE FOR Y2K
U.S. DEPARTMENT OF STATE
BEFORE THE HOUSE
COMMITTEE ON INTERNATIONAL RELATIONS
OCTOBER 21, 1999

Mr. Chairman and Members of the Committee:

Thank you for this opportunity to testify on the Year 2000 preparations by the U.S. Department of State. Those working on the Y2K problem are confronted with limited resources, limited time, imperfect information and uncertainty regarding the scope and duration of its potential effects. Despite these difficulties, the State Department has used its existing infrastructure and experience in crisis management and diplomacy to prepare for the potential impact of Y2K problems overseas. We have not done this alone, however. Work on the international aspects of the Y2K problem has truly been an interagency and multilateral organization cooperative effort, as well as a public and private sector partnership.

As reflected in the State Department's Y2K preparations, one of our highest priorities is ensuring the safety of Americans living and traveling abroad, including our own employees. We have done this by focusing our Y2K efforts in three key areas. First, we have worked to make sure that our mission-critical systems all over the world are themselves Y2K compliant so that we can continue to provide critical services to Americans overseas and domestically. The Department has fully remediated and implemented 100 percent of its Mission Critical systems deployed both domestically and internationally. Second, we have been coordinating closely with our missions abroad to ensure their continued safe operation despite any potential Y2K related disruptions in host country infrastructure. We have taken similar back-up precautions for our domestic facilities. Third, we are engaged in a dialogue and continue to cooperate with other countries to encourage their efforts to prepare for Y2K.

The Department's program to ensure Y2K compliance and the continuity of the Department's business processes includes intensive technical review, end-to-end testing and independent Y2K certification with oversight from the Office of the Inspector General for Mission Critical systems. Based on the effective implementation of our program, we have received a grade of "A" for our systems readiness from the House Subcommittee on Government Management, Information and Technology.

In addition, the Department is in the process of exercising its remediated systems to ensure that its business processes are maintained in the event of any Y2K failures. We are testing transaction flows across the major business functions, applications and infrastructure which support those transactions. For systems testing purposes, these business processes were divided into five clusters (1) Consular; (2) business management; (3) e-mail; (4) command and control communications; and (5) security. Four of the five test series have now been finished.

The remaining cluster, business management, is the most complex of the business systems being tested. This cluster includes financial, logistic and personnel systems, as well as connections with some of the Department's partners, including the Treasury Department and the Department of Commerce. We are well along in this effort and testing should be completed by the end of October.

In addition to systems readiness, our posts have taken numerous steps to ensure that their core functions, including the protection of American citizens, can continue uninterrupted. Posts have a long history of using existing emergency plans and response infrastructures for reacting to a variety of crises. We have used this existing planning infrastructure as a base and modified it to reflect some of the unique challenges posed by Y2K.

Preparations overseas have followed a multi-phased approach. In February of 1999, all posts received a Contingency Planning Toolkit to assist in their planning for the rollover. The toolkit was designed to help posts identify any gaps in existing post contingency plans and resources for potential Y2K related infrastructure problems. By May of 1999, all Chiefs of Missions certified post readiness for the transition to the Year 2000 and identified resources required to ensure operational readiness for 15 to 30 days. Based on this information, the Department prepared a request and received some funding for generators and fuel, in addition to funds for systems remediation.

The final, critical, element in the post contingency planning strategy is the contingency plan validation process. Using a web-based tool organized by Post business processes, posts are consolidating previous toolkit responses, pre-existing post emergency planning and guidance from the Department into a standardized format for a Y2K contingency plan. The key functional areas covered include diplomatic functions, consular operations, staff support functions, and security. By October 27th, posts will complete the contingency plan validation process on-line. For each business process, posts will provide the risk mitigation plan, contingency plan procedures, contingency plan testing and risk assessments.

This consolidation and standardization will allow the Department to validate each post's preparations. Post Y2K contingency plans will be reviewed against set criteria and potential problem areas identified. We will provide appropriate remedial assistance as necessary. In addition, the consolidated plans will allow those working in the Department to support Posts with any Y2K related problems during the rollover and beyond. Based on information available to date, the Department does not plan on closing any posts.

Preparation of our domestic facilities has been equally thorough. The Department has inventoried operating equipment in all of our buildings—23,000 items from elevators to pumps, lights, fans, and valves—and verified reliability with manufacturers, GSA, and our own experts. Corrective action has been taken where necessary and our building systems will operate. We have identified emergency back-up capabilities and developed contingency plans should the local power grids fail. The plans are multi-tiered, from simply protecting government assets in non-critical facilities to maintaining essential operations at critical facilities.

Our preparation to ensure the safety of Americans overseas who may face risks from Year 2000 failures has been extensive. Our efforts have focussed on providing information to the public, being open about our preparations, and ensuring back-ups for key Consular Services. In January 1999, we began our effort to educate the traveling American public about the potential for Y2K-related disruptions abroad with the issuance of a Worldwide Y2K Public Announcement. The Announcement alerted traveling Americans to the Y2K phenomenon in general and its potential to disrupt travel.

A subsequent July Public Announcement highlighted the need for personal preparedness on the part of private Americans in areas such as health-related issues and noted the inability of our missions to provide food, water and shelter to the millions of Americans abroad. The July Public Announcement also apprised the public of the measures we have taken to keep our embassies and consulates functioning. We are encouraging U.S. Citizens resident abroad to take, at a minimum, the same types of precautions as recommended by FEMA and organizations such as the Red Cross. Copies of the January and July Public Announcements are attached.

On September 14th, the Department issued updated Consular Information Sheets for every country in the world. I am pleased to provide you a summary of our country-by-country Y2K Consular Information Sheet segments (see attachment). Each Consular Information Sheet contains a section assessing the potential for disruptions, remediation efforts and possible impact in a specific country. Our fundamental purpose in releasing this information is to apprise U.S. citizens of potential disruptions they might experience due to the Y2K phenomenon, and to allow Americans to be better prepared and to make informed personal decisions about travel on or about January 1, 2000.

The Consular Information Sheets represent our best current judgment on potential problems for U.S. citizens living and traveling abroad. As we receive significant new information regarding a country's preparedness, we will provide updates. The Consular Information Sheets and future updates may be found on our website http://travel.state.gov.

At the end of October, we anticipate issuing strengthened Consular Information Sheets for a small number of countries which have not made the anticipated progress on their remediation efforts. Furthermore, if any authorized departure decisions are made for non-emergency personnel at posts, the U.S. public will be notified in the form of a Travel Warning immediately.

Our outreach program has also included speakers, media interviews and publications. Our embassies, consulates, and U.S. regional passport agencies have supplemented these efforts with "town meetings" and newsletters. In addition to outreach efforts, contingency planning has been an integral part of each and every one of our Y2K consular management efforts. Our embassies and consulates are prepared to assist American citizens to obtain relief in emergency situations. Plans have been put in place to concentrate our consular personnel and resources on providing assistance to American citizens. Each of the systems which normally support our services to American citizens have been certified Y2K compliant, but, nevertheless are backed up by two or more contingency mechanisms.

For example, we have identified alternative means of communicating with the American community in the event of power or telecommunications disruptions. Our embassies and consulates have identified local resources for food, water and shelter in the American communities abroad and sources of help from foreign governments. We are prepared for increased demand for our financial assistance program and have made contingency plans for that eventuality. Our posts have consulted with local hospitals, air ambulance services and other medical resources to identify the availability of health services in the event of disruptions.

Finally, if serious Y2K disruptions occur, we will prioritize consular services to American citizens, focusing in particular on evacuations, if necessary; medical emergencies; welfare and whereabouts inquiries; and deaths. We have coordinated with other U.S. government agencies, including INS, HHS, SSA, FEMA and DOD regarding emergency services for Americans abroad during the rollover period.

A key factor influencing our ability to support Americans abroad is the receipt of timely information. At the State Department, we plan to have our posts overseas report at one hour after midnight local time. In these "weathervane" reports, posts will be asked to comment on the status of critical infrastructure within a host country, including power, transportation, finance, water and wastewater, emergency services, telecommunications, and the impact of any disruptions on U.S. citizens. This reporting will also serve as an early warning system for the U.S. on the types of problems that may occur domestically, e.g., power grid failures or telecommunications systems degradation.

Following this initial reporting, posts will be asked to answer more detailed questions regarding the status of critical infrastructure in the host country by 12-noon local time on January 1st and every 24 hours thereafter, or if needed more frequently. We have developed specialized software that consolidates post results and depicts the local status graphically. This software supplements the already established reporting procedures through which our posts report crises to our Operations Center.

On September 9th, the Department successfully tested its ability to gather, analyze and disseminate global Y2K information in an expedient and accurate manner. This represented the most comprehensive worldwide Y2K reporting exercise within the U.S. Government. We received reports from 163 embassies and two consulates. The reporting schedule used for posts during the exercise is attached. With regard to information sharing on January 1st and the days immediately following, we will continue to work with the Information Coordination Center (ICC) of the President's Council on Year 2000 Conversion, other U.S. government agencies engaged in similar tracking of Y2K events, and the UN sponsored International Y2K Cooperation Center based at the World Bank.

We have also established a Y2K Working Group within the Department that will serve as the coordinating body of Y2K events during the rollover. This group received specific training for Y2K, and coordinated the analysis and response to information from posts abroad during the September 9th exercise. It continues to work with individual Department bureaus to establish staffing and Bureau Response Plans for the rollover. The structure of the Y2K Working Group is based on the existing infrastructure at the State Department for task forces which are convened in response to major crises abroad.

The United States does business with, and U.S. citizens travel to, or reside in almost all countries of the world. The Department of State has embassies and consulates in 164 nations. We are monitoring Y2K remediation progress in all countries where Y2K problems could affect these vital interests. The Department of State has been and continues to be an active participant in the collection and sharing of Y2K preparedness data. The Department has been collecting data from its posts on Y2K preparedness of their host nations and we have shared that information with interested organizations in the U.S. Government.

A trend line evident in virtually all studies, including our own, is that all of the countries with which the US enjoys close economic, trade and military relationships, have over the past year shown constant improvement in their state of Y2K readiness. Yet despite this favorable overall trend, we are continuing to focus on specific sectors that might pose problems to our interests and are seeking to obtain more information from the host governments involved.

The international Y2K Interagency Working Group (IWG) of the President's Council on Year 2000 Conversion co-chaired by the State Department and the Department of Defense is the forum in which Y2K preparedness information is used to formulate policy. The IWG has been meeting regularly since February of 1999, serving as both an information exchange and policy development body. IWG members have been involved in a number of international initiatives to mitigate the potential effects of Y2K on aviation safety, ports, nuclear power plants, small and medium sized businesses, and operational readiness of our military forces abroad.

IWG subgroup meetings held in late May and early June, and again in September, have tightly focused on specific countries and key sectors. Over 30 of these subgroup meetings have been held with interagency representation. As a result of these meetings, we are focusing much of our outreach effort in the next months primarily in the area of power, but also in the areas of transportation and telecommunications. These critical sectors have repeatedly surfaced as problem areas in countries of strategic interest to the U.S. These sectors have international interconnections and a failure in one country could cascade to other countries. In addition, other key sectors, such as banking and health, depend on these three sectors.

We have also worked with other APEC member countries to identify cross-border Y2K problems in the region. Similarly, we have maintained a close relationship with the countries of Africa, Latin America, the former Soviet Union and Central Europe about Y2K problems. The Department has supported the two International Y2K Coordinators' meetings held at the UN. In addition, through the G-8, we have done assessments, contingency planning and will soon coordinate our response mechanisms. In addition, we have participated in bilateral and trilateral meetings with our neighbors Canada and Mexico.

I am increasingly confident that our focused preparations, and those of other countries, have significantly reduced the potential scope of Y2K problems that the global community will have to face. However, there is no room for complacency. In the coming weeks and months, we will intensify our outreach efforts for remediation and contingency planning to focus on specific sectors within countries where we think U.S. interests might be adversely affected.

Mr. Chairman, this concludes my testimony. Thank you for the opportunity to speak to the Committee today. I will be happy to answer any questions the members may have.

Statement for the Record
House International Relations Committee

Foreign Preparedness for Y2K

Lawrence K. Gershwin
National Intelligence Officer
for Science and Technology

21 October 1999

Mr. Chairman and members of the Committee, I am pleased to have the opportunity to provide the Committee with the Intelligence Community's latest assessment of the status of foreign preparedness for Y2K. We recently published a comprehensive, classified National Intelligence Estimate on foreign Y2K efforts, and we are continuing to focus on this evolving issue to ensure that policy makers are as prepared as possible for the potential consequences for the US and our allies of international Y2K failures. This assessment is essentially a "snapshot" of the current state of international preparedness for Y2K. As countries continue their remediation, testing, and contingency planning activities, and as we get more information, some of our observations will change.

Efforts to address potential problems vary widely both among and within individual countries. For example, the United Kingdom has a highly successful government awareness campaign which has spurred industry, commerce and government agencies to take steps to correct Y2K problems. At the other end of the spectrum, when Indonesia's national electricity board was recently asked by an Indonesian newspaper about its Y2K preparedness, they replied that they can observe what happens at midnight 1999 in Western Samoa, New Zealand and Australia, and still have six hours to make plans.

- The quality of corrective work varies greatly among countries and sectors and, in some cases, remediation work introduces new flaws that go undetected due to limited or faulty testing. Moreover, time for effective corrective action is running out. Even if remediation work has taken place, there may be insufficient time left for testing, identifying problems that emerge, and follow-up remediation. Industry experts believe, in many cases, effective testing can take two to three times as long as remediation. The availability of funding and technical expertise in foreign countries to analyze vulnerabilities and carry out remediation and testing will continue to be a major impediment. The public and private sectors will increasingly focus on contingency planning for coping with the impact of Y2K failures after 1 January and prioritizing repairs.

Where effective prevention action has been taken in advance of 1 January, disruptions will likely be random, temporary, and of localized impact. In the absence of effective remediation and contingency plans, Y2K-related problems could cause widespread, possibly prolonged disruptions in vital services that could have serious humanitarian and economic consequences.

Y2K failures will occur before and as the date rollover approaches, peaking on 1 January and persisting well beyond that. In some countries, such as Russia, it will likely take a significant amount of time to overcome Y2K failures.

Russia, Ukraine, China and Indonesia are among the major countries most likely to experience significant Y2K-related failures. Countries in Western Europe are generally better prepared, although we see the chance of some significant failures in countries such as Italy. Major economic powers such as Germany and Japan are making great strides in Y2K remediation, but their late start and the magnitude of the effort suggest that even these countries are at risk of some failures. Canada, the UK, Australia, Singapore, and Hong Kong are very well prepared and have a lower chance of experiencing any significant Y2K failures.

Regional Overview

The Americas. The level of Y2K preparedness varies widely among foreign countries in the Americas and even among sectors within individual countries; Canada—working closely with the United States on sectors where national interests are highly integrated such as electrical power—emerges as the best prepared.

Most national governments in Latin America have established commissions to coordinate preparations within the public sector and to increase general awareness, but efforts in many cases are late, underfunded, and weakly enforced. Some disruptions of basic public services—including utilities, telecommunications, public health, and social welfare—are likely throughout the region, but we are unable to judge their potential scope or duration. We consider it unlikely that these disruptions will affect domestic stability or US interests in this region.

Europe. European countries, with the exception of the United Kingdom, got a late start in assessing, repairing, and planning for contingencies related to the Y2K problem. Nearly all European governments have national Y2K programs in place, and most are working very hard to minimize the significance of Y2K-related problems. However, we are concerned that some have not allotted adequate resources to remediation and testing. Remediation efforts are the most advanced in the finance and telecommunications sectors and most countries are confident major disruptions in these sectors will be avoided. Small- and medium-sized enterprises are the least prepared.

The highly integrated nature of European infrastructure and economic flows increases the risk that individual countries, even the better prepared ones, will import Y2K problems from lesser prepared neighbors.

Russia and Ukraine. Russia and Ukraine are particularly vulnerable to Y2K failures. They got a late start in remediation and lack sufficient resources to identify and correct problems--virtually guaranteeing that the countries will suffer economic and social consequences for some time. Both countries have old capital stock, much of which has not been upgraded since the Soviet era. They are further impeded because of their perception that a limited computer dependence largely "protects" them. Areas of greatest risk are strategic warning and command and control, nuclear power plants, the gas industry, and the electric power grid.

Middle East & North Africa. Most countries in the Middle East and North Africa recognize Y2K as a computer hardware and software problem, but started later in dealing with the potential problems with embedded chips and interconnected systems. The oil companies, banking sector, and large multinational companies are best informed and are conducting remediation and testing. Government institutions, small businesses, the health sector, and some public utilities lag because of funding shortfalls, a late start in addressing the problem and, in some cases, a misunderstanding of the nature and scope of Y2K vulnerabilities.

Y2K-related failures will occur, especially in public utilities, although we cannot yet judge their scope or duration. Urban areas will be most affected.

Africa. With the exception of South Africa, other countries in sub-Saharan Africa were late in recognizing the Y2K problem but are developing preparations to deal with it. Because many Africans—especially in rural areas—expect little from government, interruptions in services are unlikely to spark unrest.

Asia-Pacific. Preparations for dealing with Y2K problems across the Asia-Pacific region vary greatly. The Asian countries that rely heavily on advanced technology for power generation, communications, and transportation have had comprehensive Y2K programs under way for some time. Most countries with moderate reliance on computers are aware of potential Y2K problems and have begun assessment and remediation efforts.

The sectors with the most advanced programs for dealing with Y2K are banking and finance, civil aviation, and telecommunications. The sectors least prepared, as a general rule, are railroads, ports, medical services, and small- and medium-sized enterprises.

Impact on US of Y2K Failures

Y2K-related disruptions and failures can affect US interests in three ways:

- *They may have a direct impact.* Some foreign infrastructures and vital sectors are directly linked to those in the United States either physically or through computer networks.

- *They may have an indirect impact.* The United States depends on the uninterrupted flow of many raw materials and finished goods for its economic security and national defense. In addition, diplomatic and military operations depend upon host-nation infrastructure support, including telecommunications and electric power.

- *They may have broad national security implications.* Foreign Y2K-related crises have the potential to involve US military and civilian components in humanitarian relief, environmental disaster recovery, or evacuations.

The direct impact on the United States of Y2K-related disruptions and failures in foreign infrastructures will be limited. There are several reasons for this. First of all, Canada, the country to whose infrastructure we are most tightly linked, is well advanced in Y2K remediation and unlikely to export significant problems to the United States.

Second, the global payments system is unlikely to experience significant failures, because most of the developed countries appear well prepared in the banking and finance sector. Financial institutions in most emerging markets, however, as well as those in less developed countries, may experience failures because they started the remediation process later and because they are experiencing scarcities of resources and technical expertise.

- Even well-prepared institutions, however, will still be impacted if disruptions occur in domestic infrastructures—especially electric power and telecommunications. They are also exposed to Y2K problems in the information systems of their customers, vendors, and smaller banks to whom they are linked.

Third, we are highly confident that Y2K failures will not lead to the inadvertent or unauthorized launch of a ballistic missile by any country. If Y2K failures do occur, we are concerned about the potential for Russia to misinterpret early warning data—especially if we were in a period of increased tensions brought on by an international political crisis. Russia and the United States have agreed to establish the Center for Year 2000 Strategic Stability at Peterson Air Force Base, Colorado. The Center will provide a venue for sharing information on missile and space launches collected by US sensors across the year 2000 date change in order to prevent any misunderstandings resulting from Russian early warning failures.

Finally, the United States is unlikely to experience a significant disruption in oil deliveries because our key suppliers appear to be Y2K ready. Major multinational firms have been in the forefront of remediation and testing efforts, and operators of oil terminals and tankers have been similarly active in correcting Y2K vulnerabilities.

While we probably will not be directly impacted by foreign Y2K failures, breakdowns in foreign infrastructure could impact US interests overseas: our official and military presence overseas, US businesses, and the welfare of countries important to us. Disruptions and failures in telecommunications, electricity generation and transmission, and transportation pose the greatest threat because of their fundamental importance to all other critical services.

Sector Overview

Telecommunications. Although a high priority for most countries, efforts to remediate Y2K problems in the telecommunications sector in many countries, particularly developing countries, have been hampered by inadequate funding, a shortage of skilled personnel, a late start, and the need for lengthy remediation and testing. We estimate that only a few countries are on target in remediating and testing their telecommunications systems. Networks elsewhere are likely to experience problems ranging from minor inconveniences to serious disruptions. Experts are concerned that minor failures could cascade, causing a network to become degraded over time.

- The interconnections among many time-sensitive systems make it more likely that a Y2K problem in one system will cause problems in a system with which it is connected. Problems in telecommunications would also affect other sectors, such as power and national defense.

Failure to complete Y2K remediation is likely to result in outages that could affect the United States and foreign countries in significant ways. They could cost telecommunications operators considerable money in lost revenue; affect the operations of government, the financial sector, the military, industry, and the energy sector; and exacerbate regional tensions. Communications disruptions will damage US businesses and official activities that depend on host-government support.

Many well known companies that follow Y2K preparations list countries such as Russia, China, and Italy as likely to have telecommunications problems and we have no reason to disagree with these assessments. Some countries—such as Russia—are likely to be so poorly prepared that widespread telecommunications failures will likely occur.

Electric Power. Localized blackouts lasting possibly up to a week and regional brownouts of much shorter duration are likely to occur in Russia; however, the city of Moscow is unlikely to experience serious disruptions. In western Europe, some countries are likely to experience localized blackouts; however, a cascading failure throughout the region is highly unlikely.

- Each of the different elements of the electric power sector—generation facilities, transmission and distribution networks, telecommunications, protection systems, and consumers—forms a complex interrelationship that could cause a systemwide failure even if there were significant failures in only one element. Some electrical power grids in Europe and Asia—where Y2K remediation has been inconsistent at the national and local levels—are likely to experience outages.

Foreign Nuclear Power Plants. Y2K failures affecting nuclear power plants fall into two categories: problems that occur *outside* the nuclear plant (for example, voltage and frequency fluctuations or the collapse of the electricity grid) or, less likely, problems that occur *inside* the nuclear plant that affect generation capability. Of these two, the first is by far the more serious because nuclear plants depend on off-site electricity to operate. Loss of off-site power or large fluctuations of voltage frequency on the grid would lead to an automatic shutdown. In the event that a prolonged outage occurs, this would require, among other things, that backup systems supply power to pump coolant through the reactor core for about a week until the reactor is below fuel melting temperatures. Therefore, Y2K problems impacting generation capability in conventional plants can affect nuclear plants by causing frequency or voltage fluctuations leading to a possible collapse of the electrical grid. Similarly, Y2K problems within equipment on the grid itself might cause problems leading to the disconnection and shutdown of nuclear power plants.

We judge that those Y2K problems occurring within nuclear power plants probably will pose no direct safety problem because almost all plants have analog, electro-mechanical safety systems that will shut down the reactors if anomalies are detected. Y2K problems in digital non-safety-related systems within the nuclear plants, if they occur, would most likely lead to a reduction in generation capacity or shutdowns.

These Y2K-initiated shutdowns presumably could be conducted in a safe manner, but digital systems experiencing Y2K problems could produce false data that would then be displayed to operators, increasing the chance for operator error and, potentially, accidents. Internally-generated Y2K problems that caused a shutdown could also contribute to instability of the electricity grid by removing generation capacity from the grid. Therefore, Y2K problems at one nuclear power plant could contribute to problems at surrounding power plants.

Soviet-Designed Reactors. We are most concerned about the safety of Soviet-designed nuclear plants, including Chernobyl-type reactors in Russia and Ukraine, due both to inherent design problems of these plants—for example, lack of total containment systems—and to the lack of detailed data on Y2K remediation plans and contingency plans.

- Nonetheless, we judge the chance of a nuclear accident on the scale of Chernobyl is extremely low.

The combined effects of possible Y2K-generated internal failures and external power problems (loss of offsite power) increase the risk of a nuclear incident, particularly if operators believe they can compensate for Y2K malfunctions or for power supply reductions in the grid by overriding plant safety systems. Similar operator actions led to the accident at Chernobyl.

At this late date, remediating and testing all Soviet-designed nuclear power plant systems before yearend is not feasible, particularly given the age of the computer systems and the fact that many of the original manufacturers have gone out of business. However, countries possessing these systems have made significant efforts to identify their Y2K-related problems and are working hard to minimize the effects. Moreover, significant international attention and assistance has been beneficial.

The chance of a nuclear incident in Russia, Ukraine, or another state with Soviet-designed reactors during the Y2K rollover is low. It is, however, higher than normal because of the likelihood that the power grid could experience failures, leading to a reliance on emergency power supplies of questionable reliability, because of the possibility that auxiliary generators are inoperable due to maintenance problems or a lack of sufficient fuel, and the potential for erroneous data leading to operator error. In the worst case, this could cause a meltdown and in some cases, an accompanying release of radioactive fission gases causing localized contamination.

Gazprom Gas Deliveries. The dependence of Russian and European markets on gas deliveries from Russia's Gazprom is of particular concern. We know that several countries in Europe have extensive facilities to store natural gas and, in some cases, are preparing to increase their stored reserves in anticipation of possible disruptions in gas supplies at yearend. We cannot, however, estimate the sufficiency of these reserves should Gazprom deliveries be reduced due to Y2K failures. This would depend, in part, on the successful operation of the local pipeline distribution system. Locally severe gas shortages may occur in Russia, Ukraine, and in parts of Central and Eastern Europe due to reduced pipeline efficiency resulting from Y2K problems. Western Europe is at less risk due to greater attention to storage, contingency plans, and remediation of other infrastructure on which gas supply depends.

Transportation. Y2K problems can emerge in the transportation sector from failures in rail, highway, ports and shipping, and civil aviation services as well as from disruptions in electrical power, telecommunications, and the distribution of fuel. Because transportation systems cross national borders, noncompliance of neighbors can cause interruptions in the systems of compliant countries. Information on the potential impact of Y2K on foreign transport services and facilities has been particularly difficult to acquire, and much of it is still being gathered by international organizations and private groups. Moreover, much of the data is self-reported with little independent analysis. We lack critical details necessary to make confident judgments on problems likely to be encountered in the sector.

Commerce. Because of the increasing dependence of the US economy on "just-in-time" distribution systems, interruptions in trade flows are important to us.The lack of Y2K preparations—and even awareness—within small- and medium-sized businesses throughout the world indicates that larger enterprises, which have conscientiously addressed their own Y2K problems, may experience delays and disruptions due to failures in the systems of key business partners.

Lack of financial resources and technical skills in many cases is preventing smaller companies from undertaking remediation, and failure to take timely action will put some of them out of business.

We are also concerned about possible Y2K-related disruptions in countries planning major tourist events—for example, Italy, Egypt, Brazil, and the Caribbean—should local infrastructures experience significant failures. Other countries may experience a dramatic decline in normal tourist flows—and foreign exchange—because of concerns about Y2K-related disasters.

Implications

Public Response. Public behavior in both the runup to 1 January and in response to Y2K-generated failures, whether real or perceived, will vary widely and could have significant economic and political implications.

In developing countries, populations have minimal access to Y2K-vulnerable public services, and those who do are accustomed to frequent breakdowns. But countries with crowded urban populations could experience significant unrest if outages are prolonged.

The reactions of urban populations in developed countries are harder to gauge. Because of widespread media attention and high public awareness of the issue, we expect that the risks of panic—before and after the date rollover—are higher than in countries with lower interest in Y2K. Possible risks include hoarding, heavy bank withdrawals, safehavening financial assets, and purchases of guns and other equipment to ensure personal safety. Public reactions will depend to a great extent on how the media represents the issue. Inaccurate reporting or hyping minor inconveniences could stimulate disruptive public behavior.

We judge the threat of Y2K-inspired social unrest in developed countries to be low, but protracted delays in resolving problems with basic services, especially banks and utilities, could provoke demonstrations.

Malevolent Actors. The extensive publicity surrounding the Y2K phenomenon and the millennium, the increased vulnerability of critical infrastructures, and the resultant potential for disruptions in services could invite state and nonstate actors, including mischief-makers, to conduct attacks against the United States or US interests abroad, or against other perceived adversaries.

Humanitarian Crises. Y2K-related malfunctions have the potential to cause or exacerbate humanitarian crises through prolonged outages of power and heat, breakdowns in urban water supplies, food shortages, degraded medical services, and environmental disasters resulting from failures in safety controls. Russia, Ukraine, China, Eastern Europe, India, and Indonesia are especially vulnerable, due to their poor Y2K preparations and, in some cases, the difficulty of coping with breakdowns in critical services in the middle of winter. We are also concerned that Y2K failures in chemical plants—which are often located in urban areas—could result in environmental degradation and hazards to the nearby population.

Even the poorest countries rely on essential services that are computerized to some extent, such as power, telecommunications, food and fuel distribution, and medical care. Remediation work in these sectors, however, has proceeded slowly.

Few governments outside the West would be capable of managing widespread humanitarian needs should they arise from a breakdown of basic infrastructure in their countries, especially in urban areas. Although many have systems experienced in delivering medical and social services following natural disasters, Y2K failures present a more complex challenge because of the potential for multiple and simultaneous "disasters" within specific countries and around the world, taxing the ability of international organizations to help. Y2K failures in necessary emergency communications systems and in needed medical and social services would compound difficulties mobilizing emergency responses.

Some foreign governments and businesses will look to the United States and its better prepared infrastructure to overcome Y2K problems abroad. We expect to see "safehavening" of financial assets, routing traffic through US computer and telecommunications networks to avoid local bottlenecks, using US transportation facilities to move international trade, and calls on the US military to intervene in humanitarian crises.

Challenges for Intelligence

Y2K is a particularly challenging issue for analysis because of the uneven understanding around the world of the vulnerabilities of computer hardware and software, the unpredictability of cascading failures among interconnected systems, and the self-interest at all levels in either overstating or minimizing Y2K preparedness.

We have seen in recent months an increasing number of statements by countries and commercial enterprises that they are now prepared for Y2K, and we expect to see more such claims in the remaining three months of the year. While progress has certainly been made on many fronts, not all of these readiness claims are credible, and it is a challenge for us to sort out the truth. Commercial enterprises marketing Y2K remediation services and governments soliciting external assistance have an incentive to overstate the Y2K problem. At the same time, fear of stimulating panic, sensitivity about disclosing security vulnerabilities, and concerns about legal liability are incentives to downplay the risks of Y2K failures.

In some cases, our uncertainty about Y2K preparations in a country or sector has led us to conclude that there is an increased risk of failures. For example, in open societies with high popular interest in Y2K issues, a paucity of information about efforts to prepare public services is likely to indicate that authorities have paid insufficient attention to potential problems.

Y2K has a unique capacity to produce multiple, simultaneous crises. Its probable impact, however, is difficult to assess. We have an uneven understanding about global and national infrastructures, and the reactions of decisionmakers and the general public in a Y2K-stressed environment are also uncertain.

Furthermore, the impact of Y2K failures will depend, to some extent, on the context in which failures occur. While manageable under normal circumstances, some outages and breakdowns would assume much greater significance in the event of heightened political tensions, severe weather conditions, or an ongoing humanitarian emergency.

The Intelligence Community continues to work closely with key policy consumers to ensure that policy makers are kept informed of our best assessment of foreign Y2K developments between now and year's end.

STATEMENT OF
JACQUELYN L. WILLIAMS-BRIDGERS
INSPECTOR GENERAL OF THE
DEPARTMENT OF STATE AND
INTERNATIONAL BROADCASTING

THE YEAR 2000
COMPUTER PROBLEM: GLOBAL READINESS

BEFORE THE
COMMITTEE ON INTERNATIONAL RELATIONS
U.S. HOUSE OF REPRESENTATIVES

October 21, 1999

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to testify before the committee about our most recent analysis of global Year 2000 (Y2K) preparedness and the potential for Y2K failures in the international arena. The Y2K problem is one of the most challenging project management and systems conversion efforts ever faced by the world community. Although no one can accurately predict what will happen over the date change, we must recognize the potential for disruptions in the United States and abroad. Systems failures in countries hosting U.S. embassies, consulates, businesses, and other organizations could adversely affect the U.S. Government's ability to carry out its foreign affairs agenda and to protect U.S. interests abroad in the Year 2000. This statement addresses Office of Inspector General (OIG) oversight and review of Y2K remediation efforts by the U.S. Department of State and by countries that host our embassies and consulates.

SUMMARY

We have worked with the Department of State to assess its Y2K readiness, and that of the host countries where the U. S. maintains a diplomatic presence. Our work to date has revealed some key themes:

- Industrialized countries are well ahead of the developing world; however, some industrialized countries may have significant Y2K-related failures because they were late in establishing Y2K leadership at the national level, and because they rely heavily on computer technology in key sectors;

- Developing countries are struggling to find the financial and technical resources needed to solve their Y2K problems;

- Similar to the developing world, key sectors in the Newly Independent States and other former Eastern bloc nations are at relatively high risk of Y2K-related failures; and

- Problems related to Y2K readiness in the health sector are apparent in the majority of countries evaluated.

Our assessments have suggested that the global community will likely experience varying degrees of Y2K-related failures in various sectors, in any region, at any economic level.

In this statement I will discuss the following:

- The results of recent OIG visits to eight key countries to collect Y2K readiness information;

- The need for the Department to continue collecting information from its overseas posts concerning host country Y2K readiness and the potential for Y2K-related failures;

- The need for more detailed information on host country Y2K readiness to be made available to the public to provide a clearer picture of the potential for Y2K-related failures at foreign locations;

- The Department's progress in getting its mission critical systems Y2K certified; and

- Finally, the need for a post-Y2K assessment in order to identify lessons learned and best practices that may be applicable to government agencies and private sector organizations.

At this point, with less than 72 days to go before the Y2K transition, the Department needs to guard against complacency. In this country and around the globe a phenomenon known as "Y2K Fatigue" is beginning to occur in a public grown weary of hearing about this arcane computer problem—one that appears less real and less threatening than floods and earthquakes. Although much progress has been made and the risk of major Y2K failures appears to diminish every day, a great deal of work remains to be done in contingency planning and identifying foreign locations at high risk.

BACKGROUND

On January 1, 2000, many computer systems may malfunction or produce inaccurate information simply because of the date change. Unless prevented, these failures will adversely affect organizations and individuals around the world. Failure of host countries to resolve the Y2K problem or to create adequate contingency plans could affect U.S. interests if critical components and control systems of their infrastructure are not made Y2K compliant.

Efforts to solve Y2K problems generally have followed a phased methodology with each phase representing a major Y2K segment as described below:

- Awareness – Define the Y2K problem, obtain executive support for a Y2K program, establish a program team, and develop an overall Y2K strategy. Ensure that everyone in the organization is fully aware of the issue.
- Assessment – Determine the potential impact of Y2K on the enterprise. Inventory and analyze systems supporting core business areas and processes and establish priorities and contingency plans for their conversion or replacement. Secure the resources needed for renovation, validation, and implementation.
- Renovation – Convert, replace, or eliminate systems or components that are not Y2K compliant. Modify interfaces as necessary.
- Validation – Test and verify the performance, functionality, and integration of converted or replaced systems or components in operational environments.

- Implementation – Put the validated systems or components into production. Implement necessary contingency plans.

Under this methodology, the earliest phase, assessment, should have been completed 2 years ago, allowing sufficient time for renovation, validation, and implementation to prevent disruptions to critical business processes.

Department of State International Y2K Efforts

The Department has recognized that the potential for Y2K vulnerability is not restricted to its domestic operations and has implemented measures to assess the Y2K readiness of all countries where the United States has a diplomatic presence. These measures include the following:

- In November and December 1998, the Department's embassies and consulates used a standard survey to collect information on the effectiveness of the host country's Y2K program, vulnerability to short-term economic and social turmoil, reliance on technology in key infrastructure sectors, and the status of Y2K correctional activities. Staff under the direction of the National Intelligence Council analyzed the information from this survey, as well as from other sources, such as the World Bank, the United States Information Agency, and OIG.

- On January 29, 1999, the Department issued a Worldwide Public Announcement on the Y2K problem to inform U.S. citizens of the potential for problems throughout the world. The notice cited specific areas of concern, including transportation systems, financial institutions, and medical care, as activities that may be disrupted by Y2K-related failures. Further, this announcement warned all U.S. citizens planning to be abroad in late 1999 or early 2000 to be aware of the potential for problems and to stay informed about Y2K preparedness in the location where they will be traveling. In addition, the Department established a special Y2K website for American citizens traveling or residing abroad with links toY2K websites for foreign governments, international organizations, private organizations, and commercial enterprises at http://travel.state.gov/cay2k.

- In February 1999, the Department provided all of its embassies and consulates with a Contingency Planning Toolkit. The posts were instructed to use the toolkit to assess the probability that Y2K-related failures might occur in key infrastructure sectors, including finance, telecommunications, transportation, energy, and water/wastewater treatment. Based on this assessment, posts were to develop contingency plans and identify the resources (generators, radios, etc) needed to handle Y2K-related emergencies. As of the end of June 1999, nearly all of the Department's posts had completed their host country infrastructure assessments and developed draft contingency plans.

- In June 1999, the Department provided instructions to its embassies and consulates on how they should approach host governments concerning Y2K issues. Posts were asked to discuss with the host government its assessment of Y2K readiness in the country; gain a deeper understanding of the local authority's remedial actions and contingency plans; and inform the host government that the Department has a responsibility to notify American citizens if it is aware of credible and specific threats to their safety and security, including Y2K problems in critical sectors. The Department hoped that approaching all countries with this information would spur them to either correct the problems or develop contingency plans.

- On July 26, 1999, the Department issued a revised Worldwide Public Announcement on Y2K highlighting the need for personal preparedness on the part of private Americans and noting the inability of embassies and consulates to directly provide food, water, and shelter to the millions of U.S. citizens abroad. The Public Announcement also apprised the public of the measures the Department was taking to keep embassies and consulates functioning.

- On September 9, 1999, the Department conducted a worldwide test of its Y2K reporting system procedures. According to the Department, the test was very successful because all posts reported as scheduled. The Department plans to use this reporting system during the Year 2000 transition at the end of December.

- On September 14, 1999, the Department released updated consular information sheets containing the Department's official assessment of the potential disruptions, if any, Y2K might cause in 196 countries.

OIG Year 2000 Oversight Efforts

International Y2K Efforts: Host Country Preparedness

My office has continued its efforts in international Y2K issues by engaging host country representatives in discussions and establishing venues for information sharing and cooperation. Over the past year, we have visited 31 countries, met with host country Y2K program managers, representatives from key infrastructure sectors, and private sector officials to discuss their respective Y2K programs and shared information.

Results of Recent OIG Y2K Visits

Summarized below are the results of our most recent visits to Indonesia, China, Saudi Arabia, Egypt, Nigeria, South Africa, Brazil, and Venezuela.

- **Indonesia**: Indonesia is generally not heavily reliant on computerized systems; however, some urban centers are dependent on information technology for telecommunications and banking. Overall, the country got a late start on Y2K remediation and does not appear to be fully prepared to deal with the Y2K problem. Consequently, there is a moderate risk of Y2K disruptions across Indonesia, specifically in the key sectors of telecommunications and banking and finance. Telecommunications appears to be the sector most vulnerable to potential Y2K disruptions. Further, the banking sector's heavy reliance on telecommunications increases the risk that it may face Y2K-related disruptions. The state electrical utility has taken steps to effectively address Y2K issues; according to utility officials, they have nearly 80 percent excess power generation capacity on the key island of Java, thus making a power grid failure unlikely. There is still a possiblility of disruptions in electricity supplies due to Y2K problems in the electricity generating and distribution systems. Finally, the government has established a separate entity that will provide Y2K certification/verification assessments to systems owners.

- **China**: Major cities in the most developed region of the People's Republic of China (essentially a strip running 100 miles or so deep along the coast) are moderately reliant on computerized systems. Chinese Y2K remediation and contingency planning efforts have focused on critical infrastructure systems in these cities, which are generally well prepared to deal with the Y2K problem. Ninety percent of U.S. citizens in China live in these major cities. Little information is available concerning the Y2K readiness of China's interior provinces where, we were told, there is much less reliance on computerized systems and little potential for Y2K problems. China's power grid passed a Y2K test in early September 1999, during which power generating and transmission companies rolled through all the Y2K critical dates. Chinese authorities expect that any potential disruptions will be concentrated in small and medium-sized enterprises, and that there is a moderate risk of disruption in freight-forwarding and distribution networks.

- **Saudi Arabia**: The Kingdom of Saudi Arabia has implemented a comprehensive Y2K effort across all of its ministries. According to the July 1999, assessment by the Saudi Arabian Y2K National Committee, 100 percent of systems in the financial services and government sectors were Y2K compliant. Basic utilities were 96 percent compliant, transportation systems were at 95 percent, and telecommunications at 90 percent. The Saudi petroleum sector began its Y2K efforts in 1994 and has completed remediation, testing, and certification of its systems, except for a few medical devices used in its hospitals. The electric utility is reportedly nearly 100 percent compliant and will have 25 percent excess capacity in January 2000 because of lower usage at that time of year. In the water sector, the Saline Water Conversion Corporation has 25 plants at 15 locations around the country, producing 700 million gallons of water a day. Most of the process control devices used in these plants are analog and do not have Y2K issues. Saudi Arabia has one of the most advanced telecommunications systems in the world, according to an international U.S. telecommunications company, and it will be 100 percent compliant by October 31, 1999. Finally, according to officials at the National Committee, the health care sector has the most significant Y2K-related problems, with the government-run hospitals being the furthest behind. They are currently concentrating on contingency planning.

- **Egypt**: The Government of Egypt has implemented a centrally directed, well-organized, and comprehensive Y2K effort across all but one civilian ministry. The ministries of Interior and Defense have separate programs. The Central Bank of Egypt and the country's 54 commercial banks have completed their remediation and testing for all critical dates, including international clearing (domestic clearing is done manually). The Egyptian Electric Authority states that it has a high level of confidence in its Y2K readiness because it has fixed and tested all critical systems and embedded devices. Public hospitals, which do not expect to be compliant, are implementing a thorough risk management and staff training initiative to prepare for contingencies. The telecommunications sector is 85 to 90 percent Y2K-ready and is pursuing an ongoing Y2K program. Water and sewage treatment appear to be mostly manual operations; the U. S. Embassy in Cairo is continuing to assess these and other sectors, such as natural gas and hazardous materials. In addition, our government is strongly supporting the Egyptian Government's Y2K program. This effort includes $15.75 million in U.S. assistance targeting the power, telecommunications, health, water, wastewater, and civil aviation sectors. The Government of Egypt is setting up a national command post in Cairo that will be connected to command posts in all 26 districts that will monitor Y2K events during the rollover. Finally, the Suez Canal Authority states that it will keep the Canal clear of ships from around 11:00 p.m. on December 31, 1999, through the early morning hours of January 1, 2000. During this transition period, canal pilots will inspect shipboard navigation and other systems of transiting vessels. The Suez Canal Authority will also be checking the status of its own systems.

- **Nigeria**: Generally, the Nigerian infrastructure is not heavily dependent on computers and thus is not at significant risk of failure due to Y2K. For example, except for the Ministry of Finance, the Government of Nigeria generally uses manual systems for day-to-day activities. Much of the emphasis on Y2K remediation in Nigeria has centered on the banking and petroleum sectors. The Central Bank of Nigeria has taken some actions to assure banks continue to operate on and after December 31, 1999, including issuing Y2K compliance guidelines, and hiring inspectors and independent auditors to review and certify the Y2K preparations of the banks. However, reportedly, the Central Bank's only contingency plan is to maintain extra currency during the rollover period. The petroleum sector appears to be the best prepared. The major oil companies, including two U.S. companies, operate completely separate from the Nigerian infrastructure, and each has implemented vigorous Y2K remediation programs. For example, one company's infrastructure includes medical facilities, water/sewage plants, power facilities, office and housing compounds, drilling, pumping and docking facilities, and other structures located generally on the Nigerian coastline. The entire infrastructure of this company was checked for Y2K compliance, and systemwide testing was completed on September 9, 1999. Representatives of a second international oil company told us they tested all their information technology and embedded systems, and replaced all that were not Y2K compliant. Other key sectors in Nigeria, such as electricity, telecommunications, and air traffic control routinely experience outages, and Y2K will not likely play a significant role in determining how well they function after the rollover date.

- **South Africa**: South Africa is the most developed nation in sub-Saharan Africa and relies on computers and other automation in nearly every aspect of daily life in developed areas. An estimated $4 billion is being spent on Year 2000 programs and related contingency measures. South Africans have focused their efforts on six potentially high-risk areas: electricity, water, telecommunications, health services, transportation, and emergency services. The government currently reports the risk factor in all six areas as "low to extremely low" and expects to experience only limited disruptions through the rollover event. For example, Eskom, South Africa's electricity provider, is unlikely to experience significant outages because 1) the Y2K rollover occurs during the summer season - traditionally a low demand season; 2) most of the unit control systems at main base-load stations, as well as the country's one nuclear power plant, use analog controls; and 3) local distribution systems are electromechanical and do not use embedded logic systems. The banking sector should not experience major disruptions because the country's 60 registered banks and the South African Reserve Bank (SARB) have completed domestic and international testing and contingency planning, and SARB plans to have an extra 7.6 billion in Rand currency available to meet any increased cash demands. Although the health sector got off to a late start, the Department of Health expects all private and public health care facilities to have all their critical medical devices Y2K ready by November 30, 1999. The government is setting up a national command post in Pretoria connected to provincial command posts that will monitor Y2K events during the rollover. Finally, there is some concern that Y2K-related disruptions in other African countries might result in some refugee problems similar to those that occur when there is political instability in the region, but the government is prepared to monitor such developments carefully.

- **Brazil**: Brazil is moderately dependent on computers in its infrastructure and economy, and has made good progress in addressing Y2K problems in banking and finance, electricity, and telecommunications. In the financial sector, there has been extensive testing of all critical processes to ensure that they will continue functioning in the Year 2000. Testing included participation of over 184 financial institutions, where computer clocks were advanced to December 31, 1999, to simulate the changeover. In the electricity sector, all 72 companies in Brazil's power sector participated in an integrated test of power generation and distribution functions, and no problems were identified. Further, Brazil learned a great deal from its experience with a massive, nationwide power outage in March 1999. Even though it was not Y2K-related, the power failure provided a number of lessons learned that were incorporated into their contingency plans. Fortunately, demand for power is expected to be quite low during the Y2K rollover, thus further reducing the risk of a power failure. In the telecommunications sector, Brazil's regulatory agency has been extensively involved in ensuring Y2K compliance, and all telecommunications companies are reporting that they are Y2K compliant. The country's largest telecommunications company, Embratel, performed live tests on the network and established a central crisis center. There is less certainty about the Y2K readiness of small and medium-sized businesses and water/sewage treatment. Small and medium-sized businesses, which account for about 70 percent of the economy, started their Y2K efforts late. Many of these businesses were already suffering the continuing effects of Brazil's ongoing economic recession, thus making it even more difficult to find the financial means to resolve any Y2K problems. In the water/sewage treatment sector, there may be problems because the Y2K preparations of local governments have been mixed, and some states and municipalities that are not highly developed have not attempted to fix their systems. Finally, we were told the federal government will establish a central command post in Brasilia, and 10 regional command posts, to monitor 37 critical processes throughout the country during the rollover.

- **Venezuela**: The government of Venezuela's efforts to consolidate and take control of Y2K oversight efforts occurred only recently—September 1999. The government has hired an international consulting firm to assist it in developing a viable Y2K monitoring strategy, including mitigation strategies and contingency plans, and to evaluate the status of progress in key sectors. In addition, it is establishing an emergency response center to make countrywide decisions during the Y2K transition. The oil and finance sectors are well prepared, having worked on the Y2K issue for years. Most basic utility companies should be able to provide a normal level of service during the date change period. For example, the Caracas metropolitan area electricity provider has reportedly remediated Y2K problems in its infrastructure, production, and information systems areas. However, because utilities in rural areas have not made as much progress, there is a moderate risk of power disruption in those areas. The electricity supplier for the water sector has older equipment whose Y2K status is unknown. The telecommunications sector does not expect Y2K-related disruptions because all of its systems are reportedly Y2K compliant, but it does expect that a higher volume of calls during the Y2K transition could cause bottlenecks.

Host Country Y2K Information Flow Needs to Continue

The Department's missions have reported on their respective host countries' Y2K readiness since late 1998. This information has been used to develop contingency plans for post staff and to inform the public about potential Y2K-related failures in those countries. Further, the Department, including my office, has used this information to develop worldwide assessments of the potential impact of the Y2K problem on key infrastructure sectors (energy, transportation, communications, etc.). At the July 22, 1999, hearing, before the Senate Special Committee on the Year 2000 Technology Problem, we discussed the risks of Y2K-related failures in key sectors of industrial, developing, and Eastern bloc countries. This information was based on embassy information and our own visits.

Because the Y2K global landscape is constantly changing, it is essential that the Department continue to collect Y2K readiness information from its overseas posts and other sources. Posts are continually providing updated country assessments, and these are provided to other U.S. Government agencies and to the National Intelligence Council, which is responsible for maintaining a global Y2K database. As we enter the final 72 days of 1999, it is critical that the National Intelligence Council keep this information updated to facilitate decisionmaking on Y2K issues by U.S. Government officials both here and abroad and to keep the public informed of potential global Y2K problems.

Department Needs to Release More Detailed Y2K Readiness Information

The Department issued Consular Information Sheets for 196 countries describing Y2K readiness and the potential for Y2K-related disruptions. This ambitious and noteworthy effort to inform the public about potential disruptions abroad has focused public attention on a worldwide problem. However, based on a review of 29 information sheets, we have concerns about their adequacy. Thirteen of the 29 contained adequate Y2K information that was correct and specific enough to enable someone to make an informed decision about whether to travel to those countries. The other 16 Consular Information Sheets did not contain adequate assessments because the Y2K information provided was too vague. The Department, in its ongoing process of updating consular Y2K information, is continuously reviewing Y2K information for all countries. In particular, the Department is now focusing on possible revision of current consular information for some countries.

Some specific examples of consular information sheets that can be improved are as follows:

> **Czech Republic**: The information sheet on the Czech Republic notes that "greater progress in remediation efforts and contingency planning in rail service, electricity generation, water supply, and health care will help lower the risk of potential disruption." It would be more useful if the Department stated whether there was any evidence that such progress was being made, and whether it would be made in a timely manner.
>
> **Italy**: The information sheet is largely boilerplate and provides vague information. It should be updated to reflect more specifics regarding the current state of Y2K remediation and contingency planning to ensure that millions of travelers considering a visit to Italy for any of the planned millennium celebrations have timely, comprehensive information.
>
> **Russia and Ukraine**: The information sheets on these two countries contain strong language about the relatively high risk of potential Y2K problems, which is generally consistent with the information contained in the embassy assessments. However, despite this recognized high risk, the Department only provides a vague warning to travelers, suggesting that they "take into account fully the information in this document in planning their travel and its timing."

Over the past year the Department's embassies and consulates have provided thousands of reports to Washington concerning Y2K efforts in their respective host countries. A number of embassies, such as Embassy Beijing, have made their Y2K reporting available on their public web sites. These are linked to the Department's Y2K website at http://travel.state.gov.cay2k. The British Foreign and Commonwealth Office's travel website contains detailed, sector-specific (energy, water, etc.) Y2K information collected by British embassies in dozens of countries. These assessments and other analyses by host governments are also linked at the Department of State's website.

Some of the Department's recently issued Consular Information Sheets do not fully capture the scope and content of theY2K information collected by overseas staff, and may not, in all cases, be as useful to the American public as they could be. We recognize that in many countries information concerning the level of Y2K readiness is sensitive, given the potential impact that Y2K might have on the country's economy, its reputation, or even its internal political stability. Nonetheless, we recommend that the Department release additional information, as it becomes available, so Americans can make informed preparation if they plan to be in a foreign country on December 31, 1999.

OIG Work within the Department of State

OIG is also assisting the Department to meet the millennium challenge facing its respective information technology infrastructures, including computer software, hardware, and embedded devices. The Department has recognized that it is vulnerable to the Y2K problem, and over the past 2 years has taken steps to remediate its systems and infrastructure to prevent disruptions to its critical business processes.

The Department has established a Program Management Office (PMO) that is responsible for the overall management of the Department's Y2K program. The PMO's responsibilities include tracking and reporting on the progress being made by the bureaus in remediating systems, providing technical advice and assistance, issuing contingency planning guidance, and certifying systems for Y2K compliancy. As of May 15, 1999, the Department reported that 100 percent of its mission-critical systems had been implemented.

My office has assisted in establishing a process through which the Department can certify the Y2K compliancy of its mission-critical systems. The purpose of this process, which we understand is one of the most rigorous in the Federal Government, is to provide the Department's senior management with assurance that every feasible step has been taken to prevent Y2K-related failures on January 1, 2000. We assisted in writing detailed guidelines that each bureau must use in developing application certification packages for submission to the Y2K Project Management Office. In addition, through an agreement with the Under Secretary of State for Management, OIG is reviewing the adequacy of all certification packages for mission-critical systems before they are provided to the Y2K certification panel. Thus far, we have evaluated and provided our comments to the Department on 27 of the 54 application packages to be certified. Fourteen of the 27 have been officially certified. Another 14 certification packages are in the pipeline, and we expect to review them shortly.

Finally, in April 1999, the Department initiated planning for end-to-end testing of its core business functions. The purpose of end-to-end testing is to ensure that the Department can maintain its core business functions on and beyond the rollover to the

Year 2000. The Department's end-to-end tests of its business processes are organized around five clusters, each of which combines a number of related business functions. For example, the Business Management Cluster includes such processes as personnel actions, financial management, and logistics. The other four clusters are Consular, E-mail, Command and Control Communications, and Security. As of September 30, 1999, the Department had completed end-to-end testing of four clusters, and plans to complete testing on the fifth cluster (Business Management) by October 31, 1999.

After Y2K: What Have We Learned?

Before closing, I'd like to turn the committee's attention to the matter of what happens after Y2K, assuming the worst case scenarios do not come to pass. By January 1, 2000, organizations around the world will have spent hundreds of billions of dollars to resolve the Y2K problem. Further, organizations will spend billions more in the Year 2000 and beyond on systems that failed. There will also be the cost of post-Y2K clean up, for conducting repairs in countries that experience major outages—which we expect to be few and far between.

Some experts estimate that the total worldwide cost for Y2K, excluding litigation, will exceed $1 trillion. Given this cost, and the disruption that Y2K has produced over the past 2 years, we ask the question, what have we gained from this investment, aside from the ability to continue operations as usual? The other question is how can we avoid the next technology glitch?

I would suggest that we have much to learn from the Y2K experience. According to the Gartner Group, leading organizations encourage an after action analysis of projects in order to identify lessons learned and modify the organization's future behavior. Indeed, the collective efforts of both public and private sector organizations worldwide to resolve the Y2K problem may provide some important lessons, including best practices that may be applicable to government agencies and to private sector organizations as well. For example, the Department's project management approach to Y2K may be useful in addressing other agencywide issues, such as information security. In addition, through the laborious Y2K assessment process, the Department now has a detailed inventory of its information technology infrastructure, information that is needed for effective information resources management. Further, there are potential uses for the information collected by the Department, my office, and others on global Y2K readiness. In particular, we now have more information than ever on the extent to which countries around the world are becoming reliant on information technology.

Taking a retrospective look at Y2K may provide valuable information on what went right, what went wrong, and what we need to do in the future to either prevent another technology glitch or be better prepared when it does happen. My office is planning to address these issues over the coming year, and we would welcome any suggestions or ideas from the committee as we proceed.

CONCLUSION

Between now and the end of the year, the Department faces the difficult challenge of maintaining the momentum it has developed and keeping the world focused on the Y2K problem. Although a large part of the international community has made a great deal of progress in preparing for Y2K and developing contingency plans, much of this effort will be for naught if world leaders become complacent. The Department has a clear role to play in continuing to fine tune its own contingency plans, to collect information on host country Y2K activities, and to assure the American public is adequately informed about global Y2K readiness.

STATEMENT OF

THEODORE ALVES

**DIRECTOR, INFORMATION TECHNOLOGY AND SPECIAL AUDITS,
OFFICE OF THE INSPECTOR GENERAL,
U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT**

Y2K
COMPUTER PROBLEMS:
USAID's OPERATIONAL READINESS

BEFORE THE

**COMMITTEE ON INTERNATIONAL RELATIONS
UNITED STATES HOUSE OF REPRESENTATIVES**

October 21, 1999

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to testify before this Committee about our oversight of efforts by the U.S. Agency for International Development (USAID) to address computer related challenges that will accompany the year 2000 (Y2K). My testimony today focuses on USAID management's efforts to prepare business continuity and contingency plans that address its development assistance functions. These plans—often referred to as contingency plans—are needed to ensure that USAID will be able to continue to fulfill its mission of providing humanitarian assistance and promoting sustainable development in the event that serious Y2K problems occur. I will also describe prior Office of the Inspector General (OIG) audit results and USAID management's response and briefly cover our current efforts to verify that USAID's mission-critical systems have been adequately corrected and tested.

As we enter the new millennium, governments and private sectors throughout the world have devoted a great deal of effort to repairing computers and software programs to correctly process date related information. Although the problem is technical, involving how computers read and store dates, the solution presents a major management challenge. Computer and software defects are difficult to identify, yet, to prevent disruptions, management must identify and correct the defects; then the corrections must be successfully tested and implemented. The challenge is compounded in some developing countries that have limited technical and management capabilities.

USAID has a vital role in addressing international Y2K issues because it is responsible for important humanitarian and development assistance programs that help advance U.S. economic and political interests worldwide. USAID is the primary agency of the United States helping countries recover from disasters, escape poverty, and embrace democratic processes. USAID accomplishes its goals through its Bureaus and offices in Washington, D.C., and its Missions located in about 80 countries around the world.

SUMMARY

OIG audits have found that, after a slow start, USAID has made significant progress to mitigate the risks posed by Y2K. However, our ongoing work also shows that although USAID prepared contingency plans for key financial management business functions, it has not prepared contingency plans for some important development activities. As a result, it faces increased risks that its Bureaus and Missions could encounter operational disruptions that would limit their ability to continue providing humanitarian aid and development assistance.

These risks exist primarily because USAID has not adequately responded to two key recommendations from a prior audit report.[1] That report pointed out that USAID had not completed several steps to address Y2K challenges, including preparing contingency plans. USAID had not done so because the Y2K team lacked the authority to require Bureaus and Missions to address Y2K. The report recommended that (1) the Administrator clearly assign responsibility and authority for implementing the Y2K program, and (2) the responsible official then direct Bureaus and Missions to develop and test contingency plans. According to senior USAID officials, the Administrator directed the Bureaus to ensure that adequate plans were prepared. However, this action did not fully correct the deficiency because a single manager was not assigned the responsibility, authority, and resources to ensure adequate plans were developed.

Because little time remains to prepare for Y2K disruptions, we believe the Administrator needs to immediately (1) make a senior executive responsible and accountable, and (2) direct that manager to make sure Bureaus and Missions prepare and test business continuity and contingency plans. Because time is short, we also believe USAID needs to develop a fast track approach to quickly complete plans that focus on important development assistance activities.

[1] Audit of USAID's Assessment of the Year 2000 Problem (Audit Report No. A-000-98-006-P, September 21, 1998)

NOTABLE USAID ACTIONS

Here, I would like to briefly describe what we consider to be important USAID efforts to address the international implications of Y2K. Several of these efforts respond to deficiencies identified in our earlier audit reports. In particular, USAID has done well by:

- Recognizing the difficulties it faces dealing with Y2K issues and identifying its Y2K program as a material weakness in its fiscal year 1998 Federal Managers' Financial Integrity Act Report to the President.
- Developing contingency plans for its Washington, D.C. and Missions' financial management operations. The plans are designed to ensure that USAID has available alternative methods to perform its essential accounting functions of obligating funds, controlling funds, and making payments.
- Conducting detailed assessments of about 50 USAID Missions to identify Mission and host country Y2K vulnerabilities.
- Creating tools to help developing countries address Y2K challenges. The tools are designed to shorten or "fast-track" the process of correcting defects, preparing contingency plans, and recovering from Y2K-induced disruptions.
- Acquiring contractor services to help some Missions. As a result, some individual Missions, such as USAID/Cairo have drafted specific contingency plans that will help ensure that any Y2K problems do not severely disrupt their development activities.
- Regularly providing Y2K updates to USAID program managers. These updates provide current information about issues affecting government, private industry, and international organizations.

PRIOR AUDIT RESULTS

Now, I would like to briefly summarize OIG prior audit results and USAID's response to deficiencies we identified. USAID has been generally responsive to our reports, and has taken action to correct identified deficiencies. However, the actions taken to implement our recommendation to clearly assign responsibility and authority for the Y2K program and to develop contingency plans, did not fully correct the problems.

The OIG began oversight of USAID's Y2K activities in April 1997. Our work initially focused on USAID's efforts to complete the awareness and assessment phases as identified in GAO's Y2K Assessment Guide. These phases are designed to raise awareness of potential Y2K problems, assess the extent and severity of the problems, and identify and prioritize efforts to correct the problems. In addition, we worked to highlight the need for USAID to consider how the Y2K problem would affect its development assistance programs.

Awareness Phase: In July 1997, OIG reported [2] that USAID's plan to modify its mission-critical systems did not meet the Government-wide Y2K schedule, excluded some vulnerable systems, and placed too much reliance on the implementation of a large new financial management system, the New Management System (NMS). We found that the newly deployed system was not Y2K compliant and would encounter problems if the defects were not corrected.

We concluded that USAID executives needed to take aggressive actions to prevent problems from impairing its mission of promoting sustainable development. We recommended that USAID designate a senior management official to be responsible for Y2K, issue a Y2K program charter or policy directive, ensure that contingency plans were prepared for systems scheduled to be replaced by NMS, and inventory and assess Mission systems and non-information technology systems such as telephones and elevators.

[2] Audit of USAID's Efforts to Resolve the Year 2000 Problem (Audit Report No. A-000-97-005-P, July 11, 1997)

In response, USAID designated the Director of the Office of Information Resource Management (IRM) as the Y2K Program Manager[3], issued a Technical Team Charter, and established a Y2K project team. USAID also required contingency planning to begin for NMS and other USAID systems, and completed an inventory and assessment of Mission systems and non information technology systems.

Assessment Phase: In September 1998, we reported on USAID's Y2K assessment phase activities.[4] That report found that USAID still needed to overcome major challenges to avoid operational disruptions at the turn of the century. USAID had addressed GAO's suggested practices, but additional work was needed to complete key processes. In particular, USAID still needed to:

- Adequately identify, analyze, and prioritize systems maintained by Bureaus and Missions and systems provided to host countries with development assistance funds.

- Complete detailed schedules and resource estimates to repair mission-critical systems.

- Prepare contingency plans to ensure continuity of business operations.

We recommended that the USAID Administrator clearly assign responsibility to implement an effective Y2K program, and that the responsible official direct USAID Bureaus and Missions to develop and test contingency plans to ensure continuity of operations in the event of disruptions from Y2K problems. USAID agreed to implement our recommendations, but has not yet completely done so.

Development Assistance: In light of USAID's mission to promote sustainable development, we also invested resources to ensure that USAID considered the impact Y2K problems could have on developing countries. For example, we conducted a survey

[3] Initially, the Deputy Director of IRM was designated as the Y2K program manager.
[4] Audit of USAID's Assessment of the Year 2000 Problem (Audit Report No. A-000-98-006-P, September 21, 1998)

of Missions to analyze whether systems provided to client countries as part of their development assistance were vulnerable to Y2K problems. The survey included visiting several Missions and sending a questionnaire to all USAID Missions. The results indicated that program-funded systems were vulnerable to disruptions and that if these systems encountered problems, USAID's development assistance objectives could be adversely affected. We provided the survey results to each Bureau for review and action.

USAID's IRM office also addressed these problems by sending teams overseas, in conjunction with Bureaus, to review the status of Mission efforts to repair their systems and to evaluate risks associated with program funded and host country infrastructure systems. USAID has completed reviews at about 50 Missions, as well as coordinated with its contractors and grantees.

USAID/Philippines: A November 1998 audit report of USAID/Philippines activities found that its development assistance accomplishments had been placed at risk because the Mission had not fully addressed vulnerable program funded systems.[5] We recommended that the Mission establish a working group to address the Y2K problem for USAID-funded systems and work with the Embassy and others to develop an action plan to address the vulnerable systems. Management agreed and took action by forming a Y2K working group and developing an action plan.

[5] Audit of USAID/Philippines' Program Funded Year 2000 Sensitive Activities (Audit Report No. 5-492-99-001-P, November 30, 1998)

CONTINGENCY PLANNING NOT COMPLETE

Our current work shows that USAID faces increased risk of encountering disruptions to its development assistance programs because Bureaus and Missions have not completed contingency plans in accordance with GAO guidance. Although USAID followed GAO's guidance to prepare a contingency plan for three key financial management functions, it did not follow the guidance or prepare contingency plans for other important development assistance functions. Bureaus and Missions have not focused on preparing these plans because USAID did not fully implement our earlier recommendations to (1) clarify responsibility and authority for the Y2K program, and (2) direct Bureaus and Missions to prepare contingency plans.

USAID's Contingency Planning Activities

Recognizing that agencies faced the risk that Y2K induced disruptions could prevent them from conducting normal operations, GAO highlighted the need to prepare contingency plans to ensure the continuity of business operations. In August 1998, GAO issued guidelines that provide a good roadmap describing how to prepare contingency plans.[6] The Office of Management and Budget (OMB) also required federal agencies to use the guidelines issued by GAO to develop contingency plans and submit their Business Continuity and Contingency Plans. USAID submitted its plan to OMB on June 15, 1999.

The guide approaches contingency planning in four phases: initiation, business impact analysis, contingency planning, and testing, and provides detailed guidance for agencies to use in completing each phase. It is designed to help agencies ensure continuity of their core business processes by identifying, assessing, managing, and mitigating Y2K risks. Failure of internal information systems as well as the failures of business partners and

[6] Year 2000 Computing Crisis: Business Continuity and Contingency Planning, (GAO/AIMD-10.1.19, August 1998).

infrastructure service providers are risks posed by Y2K. The contingency planning process safeguards an agency's ability to produce a "minimum acceptable level" of outputs if internal or external systems and services were to fail. It also helps agencies restore normal service as quickly as possible and in the most cost-effective manner.

We used GAO's contingency planning guide to assess USAID's contingency planning efforts. We reviewed both the plans themselves and the process followed to prepare them. We covered the Financial Management Office and business functions in three Bureaus, reviewing studies, reports, and other documents describing the planning process and results. We also discussed the issues with responsible officials, including the Y2K program manager, the Chief Information Officer (CIO), and responsible officials in the Financial Management Office, Bureaus, and Missions. Our work was conducted from March to October 1999 in accordance with generally accepted government auditing standards. We obtained oral comments on a draft of this testimony and incorporated those comments where appropriate.

Development Assistance Functions Need to Be Addressed

Table 1 on the next page illustrates that USAID did not follow GAO's guidance for three of the four business areas we reviewed. Only the Office of Financial management had prepared a contingency plan.

TABLE I

Assessment of Contingency Planning for Selected Bureaus and Offices

		OFM	AFR	BHR	CLM
Initiation	1. Establish a business continuity project work group 2. Identify core business processes 3. Define roles and assign responsibilties 4. Develop master schedule and milestones 5. Implement quality assurance reviews	YES	NO	NO	NO
Business Impact Analysis	1. Assess the potential impact of mission-critical system failures on agency's core business processes. 2. Define Year 2000 failure scenarios, and perform risk and impact analyses of each core business process. 3. Access infrastructure risks, and define the minimum acceptable levels of outputs for each core business process	YES	NO	NO	NO
Contingency Planning	1. Identify and document contingency plans and implementation modes. 2. Define triggers for activating contingency plans, and establish business resumption team for each core business process.	YES	NO	NO	NO
Testing	1. Validate the agency's business continuity strategy. Develop and document contingency test plans. 2. Prepare and execute test. Update disaster recovery plans and procedures	PARTIAL	NO	NO	NO

YES = Completed in accordance with GAO guidelines, **NO** = Not Started, **PARTIAL** = Started but not finished

OFM = Office of Financial Management; **AFR** = Africa Bureau; **BHR** = Bureau for Humanitarian Response;
CLM = Contraceptives and Logistics Management

USAID has prepared contingency plans for key financial management functions. These functions are funds control, obligations, and payments. By having contingency plans in place for these functions, USAID has increased its assurance that it will be able to (1) control funds in accordance with Laws and regulations, (2) make funds available to award contracts and grants, and (3) make necessary payments for goods and services. USAID has not, however, fully tested the financial management contingency plans, and needs to do so to ensure that they will work as intended.

For the three development assistance business functions we reviewed, USAID has not followed GAO's suggested key steps of identifying core business processes, analyzing the risks and the possible business impact of Y2K related failures, defining failure scenarios, determining minimal acceptable levels of output, documenting contingency plans, and testing the plans. Contingency plans for important development assistance activities are needed because they represent programs that contribute significantly to advancing U.S. economic and political interests. For example:

HIV Prevention Programs: USAID-supported HIV prevention programs have reached 25 million vulnerable men and women in 45 countries. USAID reports that it has provided intensive training to nearly 200,000 counselors and educators; distributed over 1 billion condoms; and improved the clinical management of sexually transmitted infections. As a result of these programs, in Uganda, for example, USAID reports that HIV prevalence has fallen by 35 percent among young people aged 15-24.

The USAID office responsible for ordering and shipping contraceptives overseas, the Contraceptive and Logistics Management Division in the Global Bureau, has not developed and tested a contingency plan to address potential Y2K problems. Officials responsible for Y2K contingency planning told us they did not think that a contingency plan was needed for this function because suppliers and distributors usually maintain buffer stocks both in the U.S. and in Africa. However, Y2K problems could affect USAID's ability to access and distribute these stocks. Factors that could interrupt the supply chain include the inability of ships or aircraft to operate or distribution problems due to fuel shortages. Unless responsible officials follow the disciplined approach advocated by GAO to analyze the distribution problems that could occur due to Y2K problems, the program is at risk of encountering disruptions.

Humanitarian Assistance: USAID provides immediate humanitarian assistance when disasters strike. For example, USAID provides daily rations, plastic sheeting, water, and water bottles to help people to recover from natural or man-made disasters, including hurricane Mitch in Central America and population dislocations in East Timor. USAID reported that it provided 780,000 metric tons of emergency food aid, through the P.L. 480 program, to more than 11.5 million people in 28 countries in 1997. Additionally, the USAID Office of Foreign Disaster Assistance reported that it provided emergency assistance; primarily in health, sanitation, shelter, and water, totaling $140 million to help 18 million disaster victims in 46 countries. USAID may also be called on to provide humanitarian assistance to help countries recover from Y2K induced problem, yet the organization responsible, the Bureau for Humanitarian Response, has not developed and tested contingency plans for its business functions.

One responsible official told us that he did not think a contingency plan was needed because the existing arrangements are adequate. He noted that the office has agreements with contractors to supply goods, and an agreement with the Department of Defense to provide airlift capabilities if needed. However, if extensive Y2K problems develop, the Bureau might be called on to respond at a time when these support services might not be readily available. Following GAO's disciplined process would help officials consider how to deal with potential problems such as inadequate supplies for victims, unavailable transportation, or a shortage of human resources to deliver the supplies. As an indicator that transportation problems could affect supply routes, on September 9, 1999, the Coast Guard restricted the operations of 175 U.S. ships and 85 Port facilities because it did not have adequate assurance that their Y2K risks had been resolved.

Africa Bureau Operations: The Africa Bureau is responsible for managing USAID programs in Africa. The Bureau carries out the bulk of its development activities through over 20 Missions and operating units in Africa. These facilities ensure that activities supporting key USAID goals such as Infant and Child Health and Nutrition; and Agricultural Development and Food Security, are properly implemented. USAID reported that in 1998 alone its activities helped save the lives of five million children in 33 countries worldwide. Yet the Africa Bureau has not prepared a contingency plan to ensure that USAID programs in Africa are not disrupted by Y2K problems.

A Bureau official responsible for Y2K contingency planning told us he does not believe a contingency plan is necessary because the low level of automation in Africa will result in only limited problems. However, the World Bank official responsible for Y2K issues in Africa recently stated that, although the level of automation is low in Africa, the impact of Y2K problems on African societies could be severe.

USAID officials have also relied heavily on the post contingency plans developed in coordination with the U.S. Embassies around the world to provide assurance that its Missions are ready to deal with Y2K problems. While these plans should help ensure the safety and security of USAID personnel overseas, they do not address USAID's development assistance programs. We reviewed Post contingency plans for USAID Missions and other operating units in Africa and found that, of the 20 plans we reviewed, none covered USAID specific business functions.

Some Organizations Recognize Need For Contingency Plans

One Bureau and several individual Missions have recognized the need to develop contingency plans to ensure that their development assistance programs are not severely impacted if Y2K causes major disruptions. Working with the IRM Office, the Bureau for Europe and Eurasia (E&E) has procured necessary equipment and services to ensure that USAID internal systems at USAID Missions in Bulgaria, Ukraine, Hungary and Russia are Y2K compliant. The IRM Office and the Bureau have also developed concise contingency planning guidance that has been provided to program managers and other organizations responsible for implementing USAID development assistance programs at these Missions. Finally, both the Y2K committees at the Missions and the IRM office in Washington are monitoring progress.

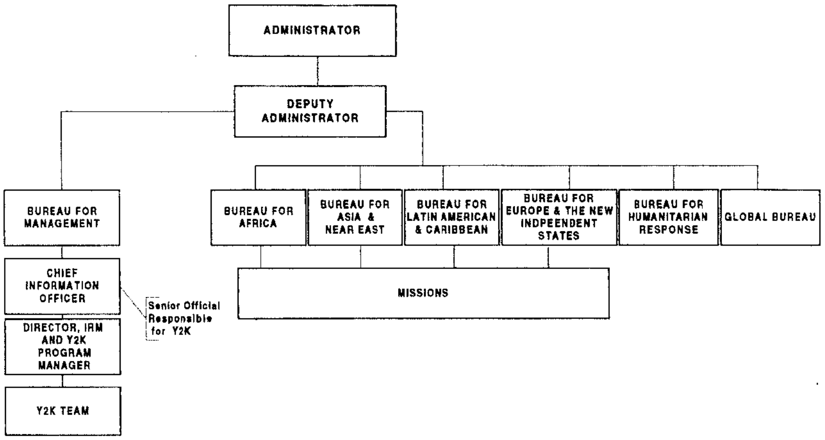
The USAID/Egypt Mission has also recognized the need to prepare contingency plans following GAO guidance. USAID/Egypt drafted a high level Y2K contingency plan that does address development assistance programs in Egypt. USAID/Egypt reported that 54 Mission employees, 350 USAID Y2K contractors, and over 100 other public and private entities participated in its efforts to identify and address anticipated Y2K problems in Egypt. The Mission now plans to develop detailed contingency plans to support its core business functions. The plan also calls for the creation of a Y2K Command and Control Center where essential staff will monitor the infrastructure during the Y2K transition.

Unclear Responsibilities Cause Problems

These problems occurred primarily because USAID has not adequately responded to two recommendations from our September 1998 audit report. In it, we reported that Bureaus and Missions were not actively engaged in efforts to (1) ensure that USAID systems would operate in the year 2000, (2) assess whether the failure of program-funded systems would adversely affect development assistance objectives, and (3) prepare contingency plans that address USAID's core business functions.

Bureaus and Missions were not more engaged in the project because the Y2K team did not have adequate authority to require other organizations to address Y2K issues. The Y2K team, which is located in the IRM office, reported through the Y2K Program Manager to the Chief Information Officer (CIO). The CIO, the senior official responsible for the Y2K effort, was organizationally located in the Management Bureau and did not have authority to direct Bureaus and Missions. The following organization chart describes the structure for USAID's Y2K program and illustrates that the Y2K team lacked authority to direct Bureaus and Missions.

USAID/YEAR 2000 ORGANIZATIONAL CHART


ADMINISTRATOR
DEPUTY ADMINISTRATOR
BUREAU FOR MANAGEMENT
CHIEF INFORMATION OFFICER
DIRECTOR, IRM AND Y2K PROGRAM MANAGER
Y2K TEAM
Senior Official Responsible for Y2K
BUREAU FOR AFRICA
BUREAU FOR ASIA & NEAR EAST
BUREAU FOR LATIN AMERICAN & CARIBBEAN
BUREAU FOR EUROPE & THE NEW INDPEENDENT STATES
BUREAU FOR HUMANITARIAN RESPONSE
GLOBAL BUREAU
MISSIONS

The report recommended that the Administrator clarify the assignment of responsibility to implement the Y2K program and provide the responsible official adequate authority and resources to complete it. To address the lack of contingency planning, the report recommended that the responsible Y2K official direct Bureaus and Missions to develop and test contingency plans. According to a senior USAID official, the Administrator met with the head of each Bureau to emphasize the importance of completing business continuity and contingency plans and received assurance that the Bureaus had adequate plans in place. Although this action partially addressed the recommendations, in our opinion, it did not correct the problem because USAID did not identify a single responsible manager.

GAO's Standards for Internal Control in the Federal Government emphasize the need for agencies to clearly define responsibility and authority and to establish clear reporting lines. GAO's internal control standards also require a system of internal controls to ensure that important activities are performed correctly. Without a responsible manager it is difficult to establish effective controls, provide appropriate oversight, and hold other managers accountable for results. A single responsible manager would help USAID to implement effective controls over the Y2K effort that ensure adequate resources are devoted, GAO guidelines are followed, and results meet quality control standards.

Action Needed to Complete Contingency Plans

Because little time remains to prepare for Y2K disruptions, we believe USAID needs to focus on completing contingency plans that will help Bureaus and Missions continue providing development assistance, respond to humanitarian crises, and assist developing and transitioning countries recover from Y2K disruptions.

Specifically, USAID needs to implement prior OIG recommendations to:

- make a senior executive responsible and accountable, and

- require Bureaus and Missions to prepare contingency plans for their development assistance program functions.

In addition, because time is running short, the IRM office should help by developing a fast track approach Bureaus and Missions can use to complete contingency plans.

Finally, the Financial Management Office needs to complete tests of key financial management functions.

SYSTEM TEST PROCESS NEEDS IMPROVEMENT

USAID has identified seven information systems as mission-critical. These systems support personnel operations, payroll, financial management for Washington and Missions, and loan servicing. USAID has decided to correct Y2K related defects for five systems, retire one financial management system, and outsource the loan servicing function to the private sector.

The largest system, NMS, is the primary financial management system supporting Washington operations with accounting, acquisition and assistance, budget, and operations functions. NMS has been the subject of previous OIG audits that identified extensive software defects and, based on OIG recommendations, USAID has decided to replace the system with Commercial Off-The-Shelf systems. Due to the size and complexity of the system and the large number of defects, the system has encountered repeated delays completing Y2K repairs. It is scheduled to be implemented by the end of October.

In its latest report to OMB, USAID stated that the remaining four systems are ready to handle Y2K dates, having been successfully tested and implemented. To provide USAID management additional assurance that these systems have been adequately repaired and tested, the OIG has been reviewing documentation describing the actions taken to correct software problems and test systems that have been implemented. The OIG obtained technical assistance from a contractor to validate the systems' readiness. We have completed reviews of two systems, the personnel system and Mission financial management system and we are in the process of reviewing the remaining three systems. The work was performed in accordance with Generally Accepted Auditing Standards, using guidelines established by GAO.[7]

[7] Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, November 1998)

Our review of the two systems disclosed that:

- Tests of Y2K dates for the personnel system were incomplete. For example, USAID's test plan identified seven Y2K dates that needed to be tested, but only three were actually tested.

- Proper testing documentation was not maintained for the Mission financial management system. According to USAID officials, tests were completed, but the testers did not maintain documentation to support the test results. This raises concerns about the adequacy of the testing process and reduces management's assurance that the system will correctly process all Y2K dates.

USAID has been very responsive to these findings and has generally taken action to correct deficiencies as they are identified. For example, based on testing deficiencies we identified in the personnel system, USAID plans to re-test a portion of the system. For the Mission financial management system, USAID will re-test a statistically valid sample of the original tests to confirm that those tests were satisfactorily completed. In addition, USAID officials have discussed the process deficiencies with the contractor officials who performed the tests. Those officials have committed to correct the problems.

CONCLUSION

In conclusion Mr. Chairman, USAID has made significant progress addressing the Y2K challenge, but needs to now focus its attention on developing business continuity and contingency plans in order to ensure that its important humanitarian and development assistance activities will not be disrupted.

This concludes my remarks and I will be pleased to answer any questions you or members of the Committee may have.

United States General Accounting Office

GAO

Testimony

Before the Committee on International Relations, House of Representatives

For Release on Delivery
10:00 am
Thursday
October 21, 1999

YEAR 2000 COMPUTING CHALLENGE

State and USAID Need to Strengthen Business Continuity Planning

Statement of Linda D. Koontz
Associate Director, Governmentwide and
Defense Information Systems
Accounting and Information Management Division

GAO
Accountability * Integrity * Reliability

Mr. Chairman and Members of the Committee:

Thank you for inviting me to participate in today's hearing on the State Department's and the United States Agency for International Development's (USAID) efforts to address the Year 2000 (Y2K) technology problem. The Y2K problem has represented a unique challenge for State and USAID. First, like all organizations, these agencies need to remediate internal computer systems and plan for unexpected disruptions within the U.S. Unlike others, however, they must also assess the Y2K status of virtually every country where the U.S. has a diplomatic presence and ensure the continuity of vital operations, such as protecting the welfare of millions of U.S. citizens traveling and living abroad, promoting economic development, providing humanitarian assistance, and achieving diplomatic agreements.

Today, I will discuss State and USAID's efforts to increase worldwide awareness of the Y2K problem, assess international preparedness, and inform American citizens of risks. In addition, I will discuss these agencies' reported progress in remediating their internal computer systems and their efforts to prepare business continuity and contingency plans to ensure that they can continue to provide critical services. To perform our work for this Committee and prepare for this testimony, we reviewed key documents and interviewed senior State and USAID officials responsible for addressing international Y2K risks. A detailed discussion of our objectives, scope, and methodology for this review is attached to this statement.

In brief, our message today on State's and USAID's efforts is a mixed one. The two agencies have taken a number of positive steps to address international Y2K risks. Through its leadership of the President's Year 2000 Council International Relations Working Group, the State Department has worked to increase awareness of the problem throughout the world, collected and shared information on the problem with other federal agencies and foreign nations, and encouraged the remediation of faulty computer systems. State has also undertaken efforts to help ensure that Americans traveling and living abroad are informed about Y2K. In addition, State has successfully tested its ability to collect and analyze information from its worldwide posts during the rollover. Similarly, USAID has devoted resources to assessing what Y2K problems could occur at many of its worldwide missions and on USAID-funded projects currently underway within the countries where these missions are located.

Both agencies also report that they have completed or almost completed remediation and testing of their mission critical computer systems. State reports that all 59 of its mission critical systems are Y2K compliant and according to USAID, 6 of 7 are compliant. USAID's New Management System is still being repaired and the agency expects it to be compliant by the end of this month.

However, State and USAID have been much less effective in the area of business continuity and contingency planning (BCCP). Because of the nature of the Y2K problem, organizations must first identify core missions and processes, decide which ones need to continue in the event of a Y2K-related emergency, and subsequently develop and test continuity and contingency plans that are clearly tied to the continuity of core processes. This is especially true for State and USAID since it is now clear that some countries will not be able to renovate all of their systems, and consequently may experience disruptions in critical services such as power, water, and finance—disruptions which, in turn, are likely to affect the operations of many embassies, consulates, and missions. Our review showed that State's BCCP did not identify and link its core business processes to its Y2K contingency plans and procedures and that the department has not yet tested its plans in Y2K-specific scenarios. USAID identified one core business process – financial management – in its Y2K BCCP, but did not identify or address other key agency functions. USAID also provided very little information on contingency planning activities for its missions and it is unclear when the agency expects to complete its BCCP process. Consequently, both agencies lack assurance that they can sustain their worldwide operations and facilities into the new millennium.

STATE AND USAID HAVE INCREASED AWARENESS OF Y2K RISKS AND ASSESSED INTERNATIONAL PREPAREDNESS

In recognition of the challenge Y2K presents, State and USAID launched comprehensive efforts to mitigate potential disruptions both here and abroad. The agencies have implemented the following initiatives to foster better awareness and gauge the likely severity of the problem.

- The State Department chairs the International Relations Working Group (IWG) of the President's Council on Year 2000 Conversion. The group has worked with other federal agencies and international organizations including the United Nations, World Bank, and International Civil Aviation Organization to increase foreign nations' awareness and encourage systems remediation by collecting and analyzing data on countries' preparedness, sharing information, supporting and attending conferences, and conducting and encouraging Y2K exercises.

- As part of the IWG's data collection efforts, State's embassies and consulates conducted surveys in late 1998 of their host countries' Y2K programs. They specifically focused on the countries' status of Y2K remediation efforts, dependence on technology in critical infrastructure sectors, and vulnerability to short-term economic and social turmoil.

- State's Inspector General's (IG) Office has collected Y2K information during overseas visits and helped oversee the department's Y2K efforts. Over the past year, IG staff visited 31 countries and met with host country representatives to increase opportunities for information sharing and cooperation. State's IG Office collected and shared with other federal entities a great deal of information on the status of foreign countries' preparedness for the Y2K rollover.

- USAID teams visited 49 of the agency's 79 overseas missions to promote awareness of the Y2K issue, assess the missions' Y2K preparedness, assess Y2K compliance of current USAID-funded IT projects, and evaluate host country Y2K vulnerabilities. The teams issued Y2K compliance evaluation reports from July 1998 through April 1999 that documented their findings and provided a baseline for remediation and contingency planning efforts. The reports vary in content but collectively indicate what USAID-funded projects are underway, whether they are computer dependent and vulnerable to Y2K problems, what their Y2K compliance status was at the time of the review, and whether the United States government, vendor, or host country is responsible for remediating the project. For example, USAID's Year 2000 Compliance Evaluation for its Cairo mission discusses the agency's portfolio of major development projects, including the installation of telephone lines and switches, disease prevention efforts, and power control centers within Egypt. Since conducting its evaluations, USAID has focused its limited resources on resolving problems in selected countries of strategic importance and/or with known Y2K vulnerabilities. According to USAID officials, the reports have also been provided to host countries' governments so they can address the findings.

- USAID developed a toolkit which foreign governments at all levels (local, provincial, and national) can use for Y2K contingency planning. USAID plans to distribute the toolkit beginning this week. According to USAID, the toolkit has been developed using a "fast-track" concept in recognition of the fact that many organizations have begun to address Y2K issues later than is optimal and that at this stage, they do not have the time to develop complete contingency plans. As such, the toolkit's design speeds the effort and reduces the resources required so that at least some contingency plans can be in place.

The collective efforts of State and USAID to analyze international Y2K readiness have shown that some countries will simply not make their Y2K deadlines and, in fact, are likely to suffer disruptions in critical infrastructure-related services such as power, water, and finance. As a result, it has become exceedingly important for State to ensure that Americans travelling and living abroad are informed about potential Y2K-related failures and that they have the best information available to help them prepare accordingly.

STATE HAS PUBLICLY REPORTED INFORMATION TO HELP SAFEGUARD AMERICANS

In implementing a broad public outreach strategy on Y2K, the Department of State issued and made available information about Y2K and foreign countries' preparedness for the millennium rollover. Much of the information is intended to help ensure that Americans living and traveling abroad, or those contemplating foreign travel on January 1, 2000, are well-informed about potential Y2K-related failures. The department's overseas posts are providing this information via numerous mechanisms, including brochures, warden[1] notices, and bulletins on post Internet home pages.

[1] The State Department's warden system consists of responsible individuals (usually U.S. citizens) in a foreign country who keep U.S. citizens in the area informed of developments during times of crisis, passing information provided to the warden by the U.S. embassy. The term "warden system" is derived from World War II when "air raid wardens" alerted citizens to emergencies. Because embassies now communicate with hundreds or thousands of citizens, the traditional warden system has evolved into a combination of telephone, fax, email, high frequency radio, media and Internet home page mechanisms.

The protection of American citizens traveling or living abroad is the department's highest priority. In recognition of this, State's long-standing "no double standard" policy requires that the department provide U.S. citizens in foreign countries with information available to official personnel regarding threats to safety and security that have not and cannot be countered. In addition, State officials have been very clear in advising U.S. citizens who may be overseas about their need to exercise personal due diligence in preparing for possible Y2K failures. As such, the department acknowledges that it does not have the resources or ability to provide food, water, shelter, fuel, or medicine to the 3 million plus Americans registered abroad or the millions more who travel for tourism or business each year. State's strategy is to provide the best possible information to Americans so that they can make their own personal emergency preparedness arrangements and informed decisions.

In January and July 1999, State issued worldwide public announcements to warn that all citizens planning to be abroad in late 1999 or early 2000 should stay informed about Y2K readiness in their respective locations. In September 1999, the department issued updated Consular Information Sheets for 196 countries which included information on Y2K related risks. The sheets are normally issued at least annually to provide advice to international travelers on issues such as a country's road conditions, crime rate, and availability of medical facilities. The current information sheets identify countries' reliance on computer systems and their level of preparedness for the Y2K problem, that is, whether they are well-prepared, prepared, generally prepared, somewhat prepared, not fully prepared, or unprepared. The sheets also assign an overall risk level (high, medium, or low) for potential Y2K disruptions in key infrastructure sectors such as energy, telecommunications, and finance, and reemphasize the need for American citizens to take precautions against Y2K-related disruptions.

However, the Y2K-related language in the current information sheets is fairly general and is not as clear as the more specific information contained in other sections of the sheet. In addition, it may be difficult for readers to distinguish the risks in one country from those in another; specifically, they may be unable to discern the differences between a country that is generally prepared from one that is somewhat prepared. State officials stated that information in the sheets on topics other than Y2K is based on past events and is not as speculative as the Y2K language. Department officials further stated that the sheets include the best Y2K-related information they had available prior to publication, but that they have subsequently obtained additional information on some countries. They stated they plan to update their website to incorporate the new information and will also do so for those countries for which new information becomes available.

In addition, the department plans to issue travel warnings later this month for selected countries if State officials determine that specific credible concerns about potential Y2K disruptions exist. Travel warnings are issued when the department decides to recommend that Americans avoid travel to specific countries. State has indicated that under its no double standard policy, travel warnings will be issued for any countries in which official personnel will be authorized to depart.

STATE AND USAID HAVE BEEN WORKING TO CORRECT THEIR INTERNAL COMPUTER SYSTEMS

The State Department has reported to the Office of Management and Budget (OMB), that all 59 of its mission critical systems[2] are Y2K compliant. In addition, State is now reporting that it has successfully completed end-to-end testing[3] of four groups of related business functions: consular, e-mail, command and control communications, and security. During this testing, State tested critical transactions throughout the department across major business areas, applications, and infrastructure that support the transactions. According to State, business management end-to-end testing is underway and expected to be completed by October 31, 1999.

According to USAID, and as reported to OMB, of its seven mission critical systems, one is not yet Y2K compliant. The New Management System (NMS)[4] is being repaired and USAID expects it to be compliant, validated, and implemented later this month. According to USAID, end-to-end testing is planned prior to the rollover, but no completion date has been established yet.

[2] Mission critical systems support business processes whose failure would seriously affect an organization's ability to meet its worldwide responsibilities.

[3] The purpose of end-to-end testing is to verify that a set of interrelated systems which collectively support an organizational core business area or function, interoperate as intended in an operational environment.

[4] NMS is a suite of administrative systems for USAID's Washington office that includes accounting, acquisition and assistance, budget, and operations functions. According to OMB, NMS has underlying implementation problems unrelated to Y2K.

STATE AND USAID BUSINESS CONTINUITY AND CONTINGENCY PLANNING EFFORTS ARE LACKING

While there has been extensive remediation and testing of mission critical systems by State and USAID, there is, nevertheless, a risk that problems may occur in the millions of lines of code that were fixed, in overlooked embedded chips, or in commercial products. There is also a risk that outside systems that exchange data with these agencies may fail as well as vital infrastructure services, such as electrical power and water. These risks, coupled with the risk of Y2K-related failures in foreign countries, mandate that agencies identify core business processes and functions, decide which ones must continue in the event of a Y2K-related emergency, and subsequently develop comprehensive BCCPs to ensure that core business processes can be continued both domestically and internationally. We have developed guidance[5] on this topic, and OMB has adopted it as the standard that federal agencies are to use in developing these plans.

Our guidance recommends a mission-based approach to business continuity and contingency planning which involves, among other steps, (1) identifying an agency's core business processes and supporting mission critical systems, (2) determining the impact of internal and external information systems, and infrastructure failures on core business processes, (3) defining the minimal acceptable level of service for each core business process, and (4) identifying and documenting contingency plans and implementation modes for each process. The guide also advocates business continuity

[5] Year 2000 Computing Crisis: Business Continuity and Contingency Planning, (GAO/AIMD-10.1.19, August 1998).

testing to evaluate whether individual contingency plans are capable of providing the desired level of support to core business processes and whether the plans can be implemented within a specified period of time.

As required by OMB, State developed a June 15, 1999, enterprisewide Y2K business continuity and contingency plan. OMB described this plan in its September 1999, quarterly report as being "too high level to determine if risks have been fully addressed." State's BCCP is a summary document which cites other supporting plans, the department's global responsibilities, and its centrally managed but decentrally implemented organizational structure. State's supporting plans include bureaus' business continuity plans, Y2K information technology systems contingency plans, Emergency Action Plans, Duty Officer Handbooks, cable guidance, and standard operating procedures.

During our review, we found that State's Y2K BCCP does not follow the mission-based approach which we recommend. The plan does not identify State's core business processes or the minimum acceptable level of service for these processes during emergency situations. State's plan also does not identify the department's mission critical systems or the impact of the failure of these systems on its core business processes. In addition, the BCCP does not link relevant contingency plans to State's core business processes and does not identify the circumstances under which these plans would apply. Finally, the plan does not indicate when or how State will test and evaluate its plans for sustaining operations in the event of Y2K disruptions. As such, the State

Department does not have assurance that it is adequately prepared to continue critical business functions in the face of Y2K failures. State officials stated that they plan to test their contingency plans across a range of functional areas, regional bureaus, and scenarios and complete these exercises around mid-November 1999. State officials also advised us that they plan to issue and resubmit to OMB a new departmentwide plan today. According to State, this revised plan appropriately links core business processes, mission critical systems, and contingency plans and meets all other OMB requirements. However, we have not had an opportunity to review this plan.

State also required that each embassy and consulate develop BCCPs, and required the head of each facility to certify that such a plan had been completed. To assist in this endeavor, State developed and distributed a Contingency Planning Toolkit in early 1999. This toolkit provided an appropriate and detailed methodology for (1) identifying critical business processes, (2) assessing the risk of systems failure, (3) assessing the risk of infrastructure failures, (4) linking existing emergency procedures to Y2K failure scenarios, (5) assessing the adequacy of existing emergency procedures and augmenting them if necessary, and (6) identifying additional resources that would be needed to execute the revised plans.

We reviewed the toolkit responses prepared by 10 embassies located in countries of particular interest to the Committee[6] and found that all were incomplete. Although most of the plans identified critical business processes as well as additional resources needed

[6] We reviewed responses from embassies in Brazil, Haiti, Indonesia, Italy, Mexico, Panama, Poland, Russia, Saudi Arabia, and Thailand.

to prepare for Y2K failures, only two linked existing contingency procedures to potential Y2K disruptions or identified any additional procedures needed. Further, there was no evidence that any of the plans had been tested. Without the kind of thorough analysis called for in State's toolkit, there is no assurance that embassies and consulates are fully prepared for potential Y2K failures. State officials agreed with our assessment, but emphasized that the department routinely deals with overseas emergencies and crises. State officials stated that their embassies have standing procedures including their Emergency Actions Plans for a variety of crises and pointed out that, on average, the department executes an evacuation every 6 weeks. State officials also stated that some posts have tested existing emergency plans in a Y2K scenario during crisis management exercises. To improve their BCCP and provide more assurance, however, State officials told us that they plan to further review and validate embassy contingency plans. As such, they stated that they have developed and implemented a web-based tool to validate posts' plans and expect to complete validation by November 11, 1999.

In addition, State is now working to determine if any authorized departures[7] from embassies will occur, due to host country infrastructure vulnerabilities. At this time, the department has declared that no posts will be closed, but that for some posts, departures may be necessary. During our review, State officials advised us that final decisions on authorized departures would be made by late October 1999 . At present, the departure

[7] According to State, when warranted in the national interest or in response to imminent threat to life, a chief of mission may request authorized (voluntary) departure status for employees in non-emergency positions and/or family members who wish to leave the post under the authorized departure option. The Department of State must issue a travel warning when either authorized or ordered (mandatory) departure is approved for official personnel and/or their families.

date for personnel at those posts selected is December 10, 1999. Case-by-case departure decisions are also being made now for selected personnel with health conditions, such as illnesses and pregnancies, due to concerns about the possibility of Y2K disruptions at medical facilities.

To further support its business continuity efforts, the department is allocating and distributing resources requested by posts to help mitigate Y2K potential problems. State officials plan for all resources to be distributed not later than December 15, 1999.

USAID BCCP Is Also Inadequate

USAID has also developed an enterprise-wide BCCP dated June 15, 1999. OMB's September, 1999, quarterly report states that "AID's plan addresses its core business functions" and that plans are in place for USAID's approximately 80 overseas posts. However, we found that USAID's BCCP is incomplete and found little evidence within the plan which would indicate that the OMB-adopted GAO methodology was followed.

USAID's BCCP identifies one core business function--financial management--and four mission critical systems supporting this function. The BCCP does not identify or address other key agency functions. Rather, the plan states that USAID is currently addressing other key processes, such as administrative services and human resources, which we believe to be support processes rather than core business processes. We also found very little information on the agency's contingency planning, including information on what alternative actions or workarounds would be taken to sustain critical operations or what events would trigger the need for these efforts. In addition, the BCCP is headquarters-focused with little information provided on mission-level contingency planning activities and provides no date for completing the plan.

Furthermore, only one mission—Cairo--has prepared a Y2K contingency plan for its specific location. USAID officials stated that despite the absence of documented BCCPs, some business continuity and contingency planning activity has been underway at USAID missions. The officials stated, however, that they could not validate the quality of or extent to which the planning activity has occurred.

USAID officials stated that financial and technical constraints have severely limited their ability to conduct effective business continuity and contingency planning. USAID's Inspector General's Office has performed a comprehensive review of its agency's Y2K business continuity and contingency planning process and efforts, and a representative from the Inspector General's office is here today to discuss the results of their work. Given the results of our and the IG's work, we are extremely concerned about USAID's ability to sustain its core business operations during the rollover and protect its overseas personnel from Y2K-related failures.

STATE IS MAKING OTHER PREPARATIONS FOR THE ROLLOVER

A significant aspect of business continuity and contingency planning is day one (also called day zero) planning. An effective day one strategy comprises a comprehensive set of actions to be executed by a federal agency during the last days of 1999 and the first days of 2000. Federal agencies and other organizations should have an effective day one strategy so they can position themselves to readily identify Y2K-induced problems, take needed corrective actions, and minimize adverse impact on their operations and key business processes. An effective day one Y2K plan will also help an agency provide information about its Y2K condition to executive management, business partners, and the public. We recently issued guidance[8] on this subject which we have provided to OMB and executive agencies for their use.

Day one planning is underway at State and USAID, although at the time of our review, it was too early to evaluate their overall efforts. We did, however, review the discussion of day one planning contained in State's current BCCP and believe the department's approach seems reasonable. State indicates it will staff the Main State building and its headquarters annexes with up to 700 employees and augment its Operations Center with additional resources in a separate Y2K response center.

[8] Y2K Computing Challenge: Day One Planning and Operations Guide (GAO/AIMD-10.1.22, October 1999).

In addition, we reviewed State's efforts to test its ability to collect and disseminate information from its overseas posts. While not required by OMB, on September 9, 1999, State conducted an exercise to test its worldwide reporting mechanisms. State selected this date because there were concerns within the computing community that some systems may interpret the "9/9/99" date as an error or as the end of a file. The objective of the exercise was to assess the department's ability to collect information on the Y2K status of all posts and host countries. No systems failed due to misreading 9/9/99. During the exercise, 165 overseas posts successfully reported status information on the impact of the 9/9/99 date rollover on operations at their facilities and host country infrastructures. State also tested its ability to assimilate and analyze this information at its headquarters location and is now assessing lessons learned for application to the actual Y2K event.

Mr. Chairman, in conclusion, the State Department has tremendous responsibilities in ensuring the safety of U.S. citizens overseas and operating its overseas posts. USAID has similar responsibilities in managing large IT-dependent projects and operating missons abroad. In addition, due to their reliance on foreign countries' infrastructures, they face challenges unique to their international missions. State and USAID will need to marshal their resources in the remaining days ahead, strengthen their BCCPs to help mitigate any Y2K-related failures, and work toward maximizing assurance that they can continue to perform their core business functions and maintain their overseas operations during the rollover. This concludes my remarks and I will be happy to answer any questions you or Members of the Committee may have.

- - - - - - -

Contact and Acknowledgement

For further information regarding this testimony, please contact Linda Koontz at (202) 512-6240 or by email at *koontzl.aimd@gao.gov*. Individuals making key contributions to this testimony include Cristina Chaplain, Kirk Daubenspeck and Brian Spencer.

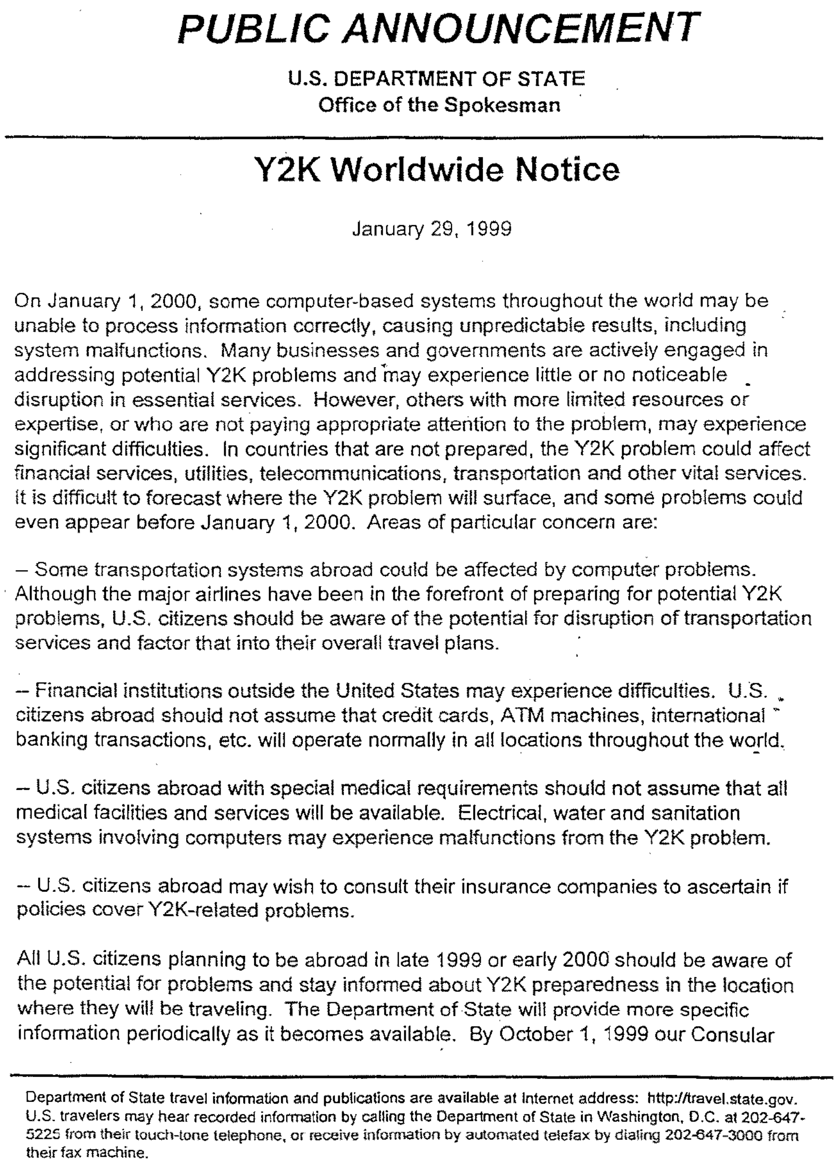
Objectives, Scope, and Methodology

To prepare for this testimony, we conducted an overview of State's and USAID's efforts to address international Year 2000 risks. We reviewed State's overall strategy for addressing the Y2K problem and ensuring the safety of Americans overseas who may face risks from Y2K-related failures. Our work at USAID focused on the agency's efforts to address Y2K-related risks to USAID-funded information technology projects and systems in foreign nations.

We reviewed a number of key documents including the State Department's enterprise-wide Y2K BCCP; analyses of foreign nations' preparedness for the Y2K problem; bureau, embassy, and systems Y2K contingency plans; selected embassy Emergency Action Plans; Consular Information Sheets; and public Y2K announcements. We also reviewed USAID's overall Y2K BCCP, a Y2K contingency plan for one mission, and about 50 assessments of selected overseas missions' preparedness and their dependence on host country infrastructures.

In addition, we interviewed senior officials responsible for addressing international Y2K risks, including the State Department's Special Representative for the Year 2000 Problem, Deputy Chief Information Officer for Y2K, Deputy Chief Information Officer for Operations, Deputy Assistant Secretary for Diplomatic Security, Deputy Assistant

Secretary for Administration, Managing Director for International Financial Services, Executive Director for Consular Affairs, Director of Overseas Citizens Services, and the Director of the Y2K Working Group. At USAID, we interviewed senior officials including the agency's Chief Information Officer and the Director, Office of Information Resources Management. We performed our work in Washington, D.C., between August and October 1999, in accordance with generally accepted government auditing standards. We obtained comments on a draft of this testimony from State and USAID officials and incorporated these comments where appropriate.



PUBLIC ANNOUNCEMENT

U.S. DEPARTMENT OF STATE
Office of the Spokesman

Y2K Worldwide Notice

January 29, 1999

On January 1, 2000, some computer-based systems throughout the world may be unable to process information correctly, causing unpredictable results, including system malfunctions. Many businesses and governments are actively engaged in addressing potential Y2K problems and may experience little or no noticeable disruption in essential services. However, others with more limited resources or expertise, or who are not paying appropriate attention to the problem, may experience significant difficulties. In countries that are not prepared, the Y2K problem could affect financial services, utilities, telecommunications, transportation and other vital services. It is difficult to forecast where the Y2K problem will surface, and some problems could even appear before January 1, 2000. Areas of particular concern are:

-- Some transportation systems abroad could be affected by computer problems. Although the major airlines have been in the forefront of preparing for potential Y2K problems, U.S. citizens should be aware of the potential for disruption of transportation services and factor that into their overall travel plans.

-- Financial institutions outside the United States may experience difficulties. U.S. citizens abroad should not assume that credit cards, ATM machines, international banking transactions, etc. will operate normally in all locations throughout the world.

-- U.S. citizens abroad with special medical requirements should not assume that all medical facilities and services will be available. Electrical, water and sanitation systems involving computers may experience malfunctions from the Y2K problem.

-- U.S. citizens abroad may wish to consult their insurance companies to ascertain if policies cover Y2K-related problems.

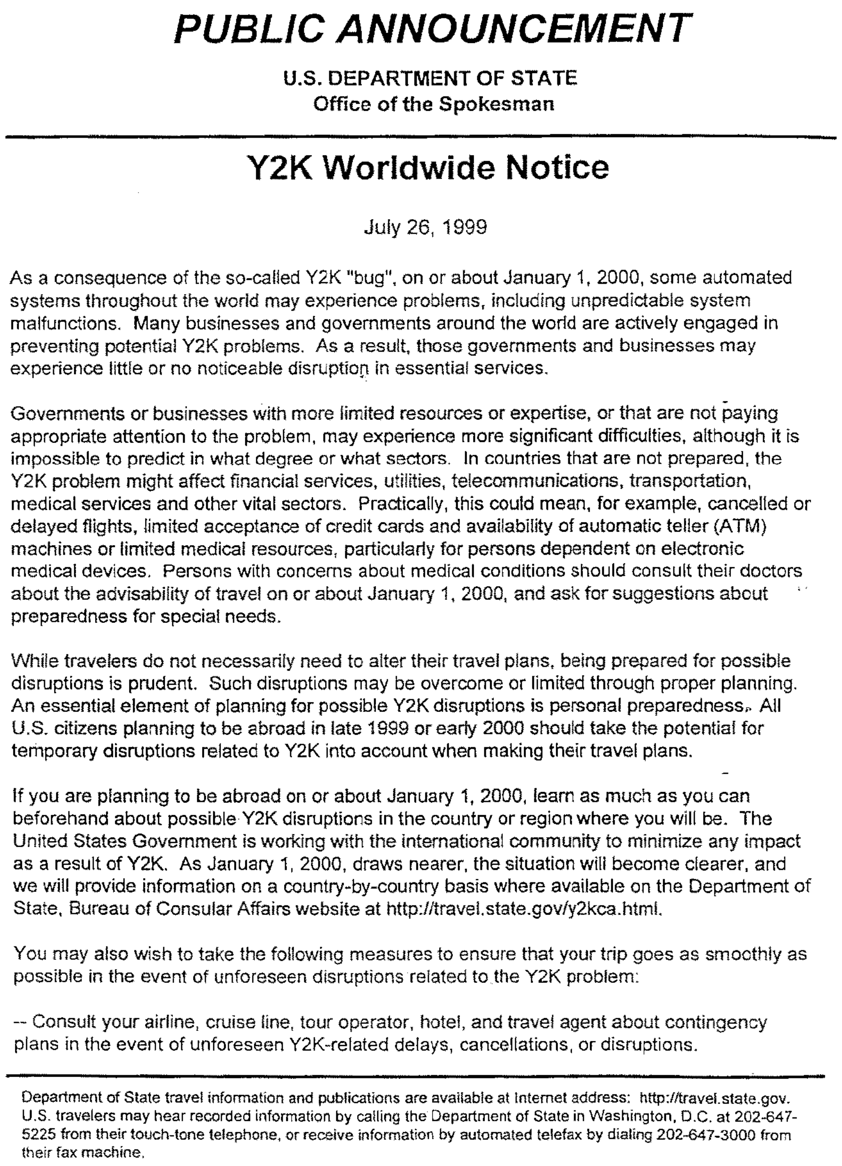
All U.S. citizens planning to be abroad in late 1999 or early 2000 should be aware of the potential for problems and stay informed about Y2K preparedness in the location where they will be traveling. The Department of State will provide more specific information periodically as it becomes available. By October 1, 1999 our Consular

Department of State travel information and publications are available at Internet address: http://travel.state.gov. U.S. travelers may hear recorded information by calling the Department of State in Washington, D.C. at 202-647-5225 from their touch-tone telephone, or receive information by automated telefax by dialing 202-647-3000 from their fax machine.

Information Sheets on individual countries will contain specific information, as available, on the Y2K preparations in each country.

These can be accessed through the Department of State, Bureau of Consular Affairs home page via the Internet at http://travel.state.gov. Monitor our home page for additional information about Y2K issues and links to Y2K web sites for foreign governments, U.S. Government agencies and international organizations.

This Public Announcement expires March 1, 2000.



PUBLIC ANNOUNCEMENT

U.S. DEPARTMENT OF STATE
Office of the Spokesman

Y2K Worldwide Notice

July 26, 1999

As a consequence of the so-called Y2K "bug", on or about January 1, 2000, some automated systems throughout the world may experience problems, including unpredictable system malfunctions. Many businesses and governments around the world are actively engaged in preventing potential Y2K problems. As a result, those governments and businesses may experience little or no noticeable disruption in essential services.

Governments or businesses with more limited resources or expertise, or that are not paying appropriate attention to the problem, may experience more significant difficulties, although it is impossible to predict in what degree or what sectors. In countries that are not prepared, the Y2K problem might affect financial services, utilities, telecommunications, transportation, medical services and other vital sectors. Practically, this could mean, for example, cancelled or delayed flights, limited acceptance of credit cards and availability of automatic teller (ATM) machines or limited medical resources, particularly for persons dependent on electronic medical devices. Persons with concerns about medical conditions should consult their doctors about the advisability of travel on or about January 1, 2000, and ask for suggestions about preparedness for special needs.

While travelers do not necessarily need to alter their travel plans, being prepared for possible disruptions is prudent. Such disruptions may be overcome or limited through proper planning. An essential element of planning for possible Y2K disruptions is personal preparedness. All U.S. citizens planning to be abroad in late 1999 or early 2000 should take the potential for temporary disruptions related to Y2K into account when making their travel plans.

If you are planning to be abroad on or about January 1, 2000, learn as much as you can beforehand about possible Y2K disruptions in the country or region where you will be. The United States Government is working with the international community to minimize any impact as a result of Y2K. As January 1, 2000, draws nearer, the situation will become clearer, and we will provide information on a country-by-country basis where available on the Department of State, Bureau of Consular Affairs website at http://travel.state.gov/y2kca.html.

You may also wish to take the following measures to ensure that your trip goes as smoothly as possible in the event of unforeseen disruptions related to the Y2K problem:

-- Consult your airline, cruise line, tour operator, hotel, and travel agent about contingency plans in the event of unforeseen Y2K-related delays, cancellations, or disruptions.

Department of State travel information and publications are available at Internet address: http://travel.state.gov. U.S. travelers may hear recorded information by calling the Department of State in Washington, D.C. at 202-647-5225 from their touch-tone telephone, or receive information by automated telefax by dialing 202-647-3000 from their fax machine.

-- Obtain written confirmation of reservations.

-- Consider purchasing trip cancellation insurance.

-- Anticipate possible delays in flights overseas. Give yourself plenty of time, if your travel itinerary includes connecting flights.

-- Make sure that your essential possessions such as passports, medications, eyeglasses, emergency telephone numbers and contacts for your place of destination and back home, etc., are in carry-on baggage. Your supply of medications should be sufficient to last for the anticipated duration of travel.

-- Consult your insurance companies to ascertain whether your insurance policies cover Y2K-related problems, including health and accident coverage abroad.

Please note that U.S. embassies and consulates abroad do not have facilities to provide private U.S. citizens overseas with food, water, fuel, medicines, shelter or other equipment and supplies in the event of disruptions of essential services in foreign countries. The Department of State is preparing its embassies and consulates worldwide for continual operation through the beginning of the new year. Our embassies and consulates will be available to assist American citizens in emergency circumstances. Nevertheless, this ability may be hampered by local Y2K disruptions. The Department of State expects to evacuate, prior to January 1, U.S. Embassy personnel who are medically reliant on systems that may not be Y2K compliant.

For additional ideas about personal preparedness, see the websites of the U.S. Federal Emergency Management Agency (FEMA) at http://www.fema.gov/y2k/, the President's Council on Year 2000 Conversion at http://www.y2k.gov, and the American Red Cross at http://www.redcross.org/y2k.

For general information about the Y2K problem abroad, see the Department of State, Bureau of Consular Affairs' pamphlet "Are You Ready for Y2K?" now available on our Y2K website at http://travel.state.gov/y2kca.html . See also the home page of the U.S. Embassy or Consulate in the country or countries where you reside or plan to visit for additional preparedness information. These can be accessed through the Department of State, Bureau of Consular Affairs home page at http://travel.state.gov. The Department of State will provide more specific information as it becomes available. Monitor our Y2K website at http://travel.state.gov/y2kca.html for additional information about Y2K issues.

This Public Announcement supersedes our Y2K Notice of January 29, 1999, and expires on March 1, 2000.

Y2K Sections of Consular Information Sheets

The Y2K sections of the Consular Information Sheets provide American citizens traveling or residing abroad with information regarding the Y2K status of specific countries. In addition to the country-specific information, the Y2K section of the Consular Information Sheet for each country provides travelers with general Y2K information to enable them to make informed personal travel decisions.

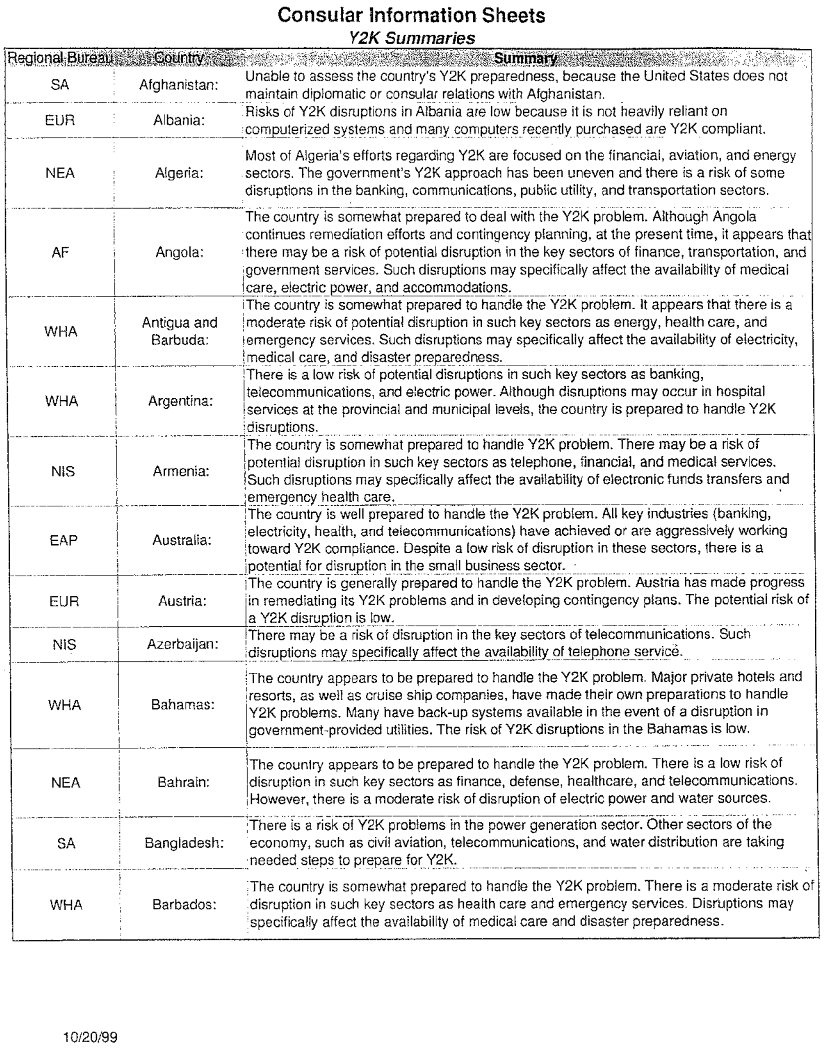
The attached document entitled, "Consular Information Sheets: Y2K Summaries," summarizes only the country-specific language found in each Consular Information Sheet. In order to provide you with a sample of the general Y2K information which is included in the Consular Information Sheets, the Y2K section from the Consular Information Sheet for Germany is provided below. For this example, the general information, including the first paragraph, is shown in bold.

> **Germany - Consular Information Sheet Y2K Excerpt**
> September 14, 1999
>
> **Y2K INFORMATION: As a consequence of the so called Y2K "bug", on or about January 1, 2000, some automated systems throughout the world may experience problems, including unpredictable system malfunctions. In countries that are not prepared, the Y2K problem could affect financial services, utilities, health services, telecommunications, energy, transportation and other vital services. American citizens who are traveling to any country during this time period should be aware of the potential for the disruption of normal medical services. Travelers with special medical needs should consult with their personal physician and take appropriate precautions. While travelers do not necessarily need to alter their travel plans, being informed and prepared for possible disruptions is prudent.**
>
> Germany is a modern industrial state dependent on computer systems for a large part of its production of goods and services. It has made progress on remediating Y2K problems, developing contingency plans, and is otherwise well prepared to deal with any Y2K-generated problems. There is a low risk of potential Y2K disruptions in key sectors. Germany is also working with the international community and its fellow European Union member states to minimize the economic impact of Y2K problems.
>
> It is, of course, difficult to predict the severity or duration of potential Y2K-related disruptions. U.S. citizens traveling to or residing in Germany in late 1999 or early 2000 should, therefore, be aware of potential difficulties and take practical precautions, anticipate the potential for disruption to their daily activities, and be prepared to cope with the impact of such disruptions. **Information about personal preparedness and Y2K is available in the Department of State Worldwide Public Announcement of July 26, 1999**

which is accessible on the Department of State, Bureau of Consular Affairs home page at http://travel.state.gov/y2kca.html.

Aviation and Y2K: The Department of Transportation is heading an international year 2000 civil aviation evaluation process to review information on Y2K readiness in aviation based on reports to the international civil aviation organization and other available sources. The Federal Aviation Administration is working with the industry and its international partners to encourage sharing of Y2K readiness and contingency planning information so that air carriers will be able to make appropriate decisions. Please consult your airline about contingency plans in the event of unforeseen Y2K-related delays, cancellations, or disruptions. Please see the Department of Transportation Y2K home page at http://www.dot.gov/fly2k for updated information on Y2K and aviation issues.

As January 1, 2000 draws nearer, we will provide updated information available to us about important Y2K issues in Germany **on the Consular Affairs home page at http://travel.state.gov/y2kca.html.** In addition, please monitor the home page of the U.S. Embassy in Berlin at http://www.usembassy.de. Please see also the Government of Germany's internet website on Y2K issues at http://www.iid.de/jahr2000/bericht2000/index_engl.html for additional updates.

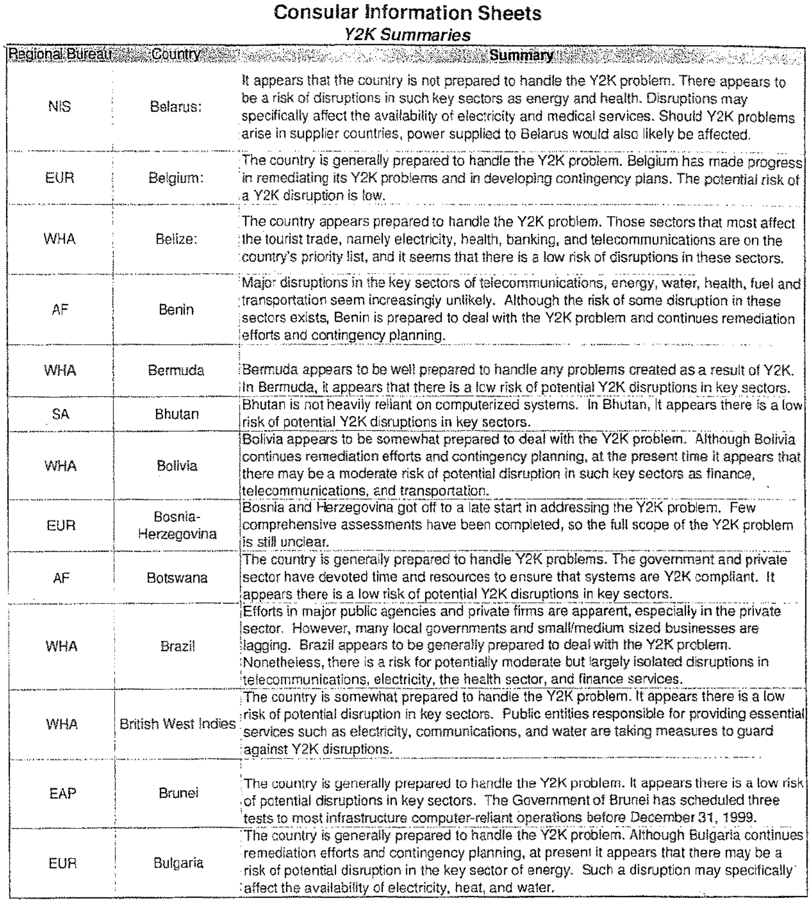


Consular Information Sheets

Y2K Summaries

Regional Bureau	Country	Summary
SA	Afghanistan:	Unable to assess the country's Y2K preparedness, because the United States does not maintain diplomatic or consular relations with Afghanistan.
EUR	Albania:	Risks of Y2K disruptions in Albania are low because it is not heavily reliant on computerized systems and many computers recently purchased are Y2K compliant.
NEA	Algeria:	Most of Algeria's efforts regarding Y2K are focused on the financial, aviation, and energy sectors. The government's Y2K approach has been uneven and there is a risk of some disruptions in the banking, communications, public utility, and transportation sectors.
AF	Angola:	The country is somewhat prepared to deal with the Y2K problem. Although Angola continues remediation efforts and contingency planning, at the present time, it appears that there may be a risk of potential disruption in the key sectors of finance, transportation, and government services. Such disruptions may specifically affect the availability of medical care, electric power, and accommodations.
WHA	Antigua and Barbuda:	The country is somewhat prepared to handle the Y2K problem. It appears that there is a moderate risk of potential disruption in such key sectors as energy, health care, and emergency services. Such disruptions may specifically affect the availability of electricity, medical care, and disaster preparedness.
WHA	Argentina:	There is a low risk of potential disruptions in such key sectors as banking, telecommunications, and electric power. Although disruptions may occur in hospital services at the provincial and municipal levels, the country is prepared to handle Y2K disruptions.
NIS	Armenia:	The country is somewhat prepared to handle Y2K problem. There may be a risk of potential disruption in such key sectors as telephone, financial, and medical services. Such disruptions may specifically affect the availability of electronic funds transfers and emergency health care.
EAP	Australia:	The country is well prepared to handle the Y2K problem. All key industries (banking, electricity, health, and telecommunications) have achieved or are aggressively working toward Y2K compliance. Despite a low risk of disruption in these sectors, there is a potential for disruption in the small business sector.
EUR	Austria:	The country is generally prepared to handle the Y2K problem. Austria has made progress in remediating its Y2K problems and in developing contingency plans. The potential risk of a Y2K disruption is low.
NIS	Azerbaijan:	There may be a risk of disruption in the key sectors of telecommunications. Such disruptions may specifically affect the availability of telephone service.
WHA	Bahamas:	The country appears to be prepared to handle the Y2K problem. Major private hotels and resorts, as well as cruise ship companies, have made their own preparations to handle Y2K problems. Many have back-up systems available in the event of a disruption in government-provided utilities. The risk of Y2K disruptions in the Bahamas is low.
NEA	Bahrain:	The country appears to be prepared to handle the Y2K problem. There is a low risk of disruption in such key sectors as finance, defense, healthcare, and telecommunications. However, there is a moderate risk of disruption of electric power and water sources.
SA	Bangladesh:	There is a risk of Y2K problems in the power generation sector. Other sectors of the economy, such as civil aviation, telecommunications, and water distribution are taking needed steps to prepare for Y2K.
WHA	Barbados:	The country is somewhat prepared to handle the Y2K problem. There is a moderate risk of disruption in such key sectors as health care and emergency services. Disruptions may specifically affect the availability of medical care and disaster preparedness.

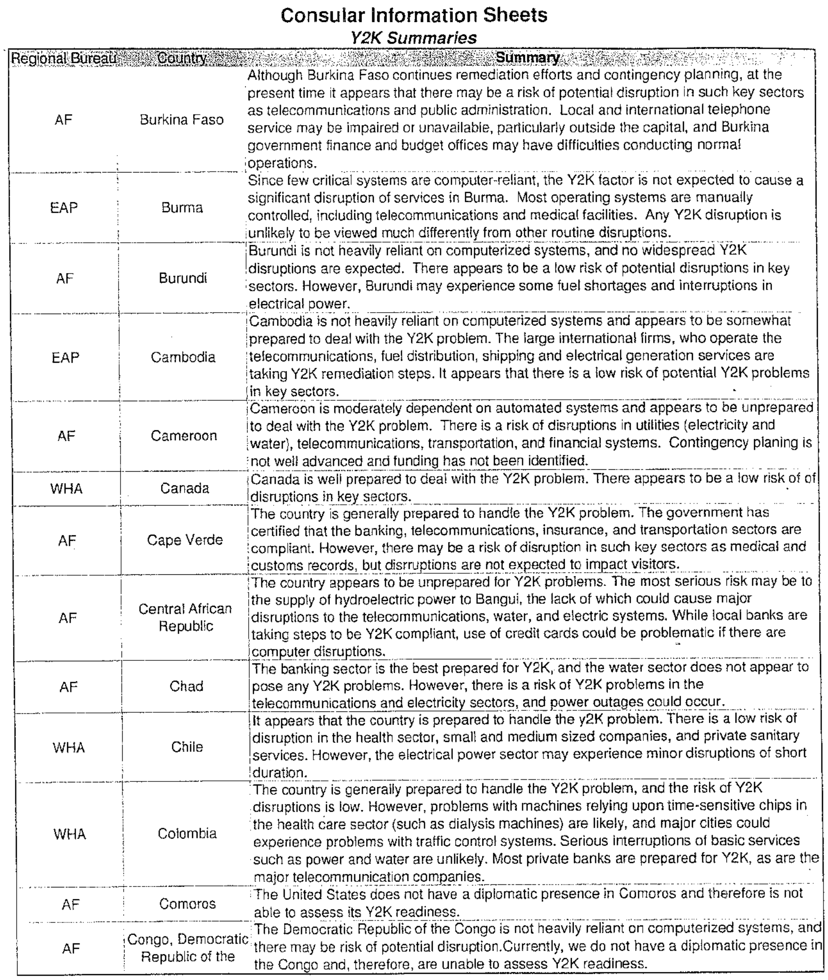
10/20/99



Consular Information Sheets

Y2K Summaries

Regional Bureau	Country	Summary
NIS	Belarus:	It appears that the country is not prepared to handle the Y2K problem. There appears to be a risk of disruptions in such key sectors as energy and health. Disruptions may specifically affect the availability of electricity and medical services. Should Y2K problems arise in supplier countries, power supplied to Belarus would also likely be affected.
EUR	Belgium:	The country is generally prepared to handle the Y2K problem. Belgium has made progress in remediating its Y2K problems and in developing contingency plans. The potential risk of a Y2K disruption is low.
WHA	Belize:	The country appears prepared to handle the Y2K problem. Those sectors that most affect the tourist trade, namely electricity, health, banking, and telecommunications are on the country's priority list, and it seems that there is a low risk of disruptions in these sectors.
AF	Benin	Major disruptions in the key sectors of telecommunications, energy, water, health, fuel and transportation seem increasingly unlikely. Although the risk of some disruption in these sectors exists, Benin is prepared to deal with the Y2K problem and continues remediation efforts and contingency planning.
WHA	Bermuda	Bermuda appears to be well prepared to handle any problems created as a result of Y2K. In Bermuda, it appears that there is a low risk of potential Y2K disruptions in key sectors.
SA	Bhutan	Bhutan is not heavily reliant on computerized systems. In Bhutan, it appears there is a low risk of potential Y2K disruptions in key sectors.
WHA	Bolivia	Bolivia appears to be somewhat prepared to deal with the Y2K problem. Although Bolivia continues remediation efforts and contingency planning, at the present time it appears that there may be a moderate risk of potential disruption in such key sectors as finance, telecommunications, and transportation.
EUR	Bosnia-Herzegovina	Bosnia and Herzegovina got off to a late start in addressing the Y2K problem. Few comprehensive assessments have been completed, so the full scope of the Y2K problem is still unclear.
AF	Botswana	The country is generally prepared to handle Y2K problems. The government and private sector have devoted time and resources to ensure that systems are Y2K compliant. It appears there is a low risk of potential Y2K disruptions in key sectors.
WHA	Brazil	Efforts in major public agencies and private firms are apparent, especially in the private sector. However, many local governments and small/medium sized businesses are lagging. Brazil appears to be generally prepared to deal with the Y2K problem. Nonetheless, there is a risk for potentially moderate but largely isolated disruptions in telecommunications, electricity, the health sector, and finance services.
WHA	British West Indies	The country is somewhat prepared to handle the Y2K problem. It appears there is a low risk of potential disruption in key sectors. Public entities responsible for providing essential services such as electricity, communications, and water are taking measures to guard against Y2K disruptions.
EAP	Brunei	The country is generally prepared to handle the Y2K problem. It appears there is a low risk of potential disruptions in key sectors. The Government of Brunei has scheduled three tests to most infrastructure computer-reliant operations before December 31, 1999.
EUR	Bulgaria	The country is generally prepared to handle the Y2K problem. Although Bulgaria continues remediation efforts and contingency planning, at present it appears that there may be a risk of potential disruption in the key sector of energy. Such a disruption may specifically affect the availability of electricity, heat, and water.



Consular Information Sheets

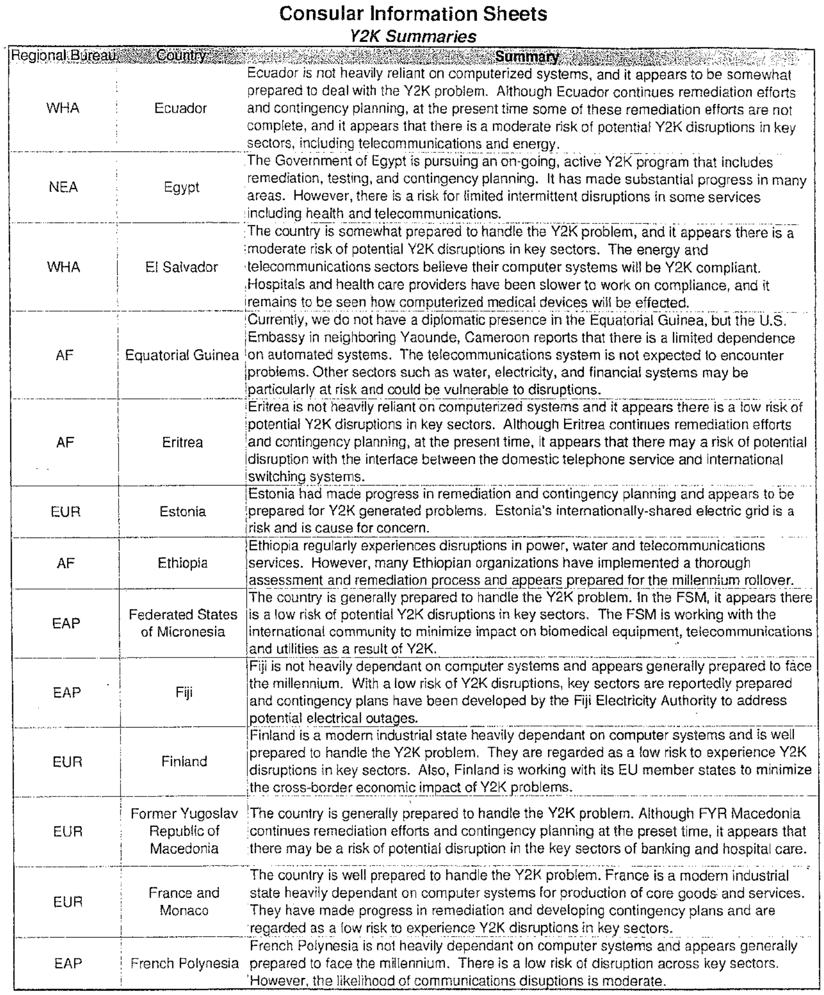
Y2K Summaries

Regional Bureau	Country	Summary
AF	Burkina Faso	Although Burkina Faso continues remediation efforts and contingency planning, at the present time it appears that there may be a risk of potential disruption in such key sectors as telecommunications and public administration. Local and international telephone service may be impaired or unavailable, particularly outside the capital, and Burkina government finance and budget offices may have difficulties conducting normal operations.
EAP	Burma	Since few critical systems are computer-reliant, the Y2K factor is not expected to cause a significant disruption of services in Burma. Most operating systems are manually controlled, including telecommunications and medical facilities. Any Y2K disruption is unlikely to be viewed much differently from other routine disruptions.
AF	Burundi	Burundi is not heavily reliant on computerized systems, and no widespread Y2K disruptions are expected. There appears to be a low risk of potential disruptions in key sectors. However, Burundi may experience some fuel shortages and interruptions in electrical power.
EAP	Cambodia	Cambodia is not heavily reliant on computerized systems and appears to be somewhat prepared to deal with the Y2K problem. The large international firms, who operate the telecommunications, fuel distribution, shipping and electrical generation services are taking Y2K remediation steps. It appears that there is a low risk of potential Y2K problems in key sectors.
AF	Cameroon	Cameroon is moderately dependent on automated systems and appears to be unprepared to deal with the Y2K problem. There is a risk of disruptions in utilities (electricity and water), telecommunications, transportation, and financial systems. Contingency planing is not well advanced and funding has not been identified.
WHA	Canada	Canada is well prepared to deal with the Y2K problem. There appears to be a low risk of of disruptions in key sectors.
AF	Cape Verde	The country is generally prepared to handle the Y2K problem. The government has certified that the banking, telecommunications, insurance, and transportation sectors are compliant. However, there may be a risk of disruption in such key sectors as medical and customs records, but disrruptions are not expected to impact visitors.
AF	Central African Republic	The country appears to be unprepared for Y2K problems. The most serious risk may be to the supply of hydroelectric power to Bangui, the lack of which could cause major disruptions to the telecommunications, water, and electric systems. While local banks are taking steps to be Y2K compliant, use of credit cards could be problematic if there are computer disruptions.
AF	Chad	The banking sector is the best prepared for Y2K, and the water sector does not appear to pose any Y2K problems. However, there is a risk of Y2K problems in the telecommunications and electricity sectors, and power outages could occur.
WHA	Chile	It appears that the country is prepared to handle the y2K problem. There is a low risk of disruption in the health sector, small and medium sized companies, and private sanitary services. However, the electrical power sector may experience minor disruptions of short duration.
WHA	Colombia	The country is generally prepared to handle the Y2K problem, and the risk of Y2K disruptions is low. However, problems with machines relying upon time-sensitive chips in the health care sector (such as dialysis machines) are likely, and major cities could experience problems with traffic control systems. Serious interruptions of basic services such as power and water are unlikely. Most private banks are prepared for Y2K, as are the major telecommunication companies.
AF	Comoros	The United States does not have a diplomatic presence in Comoros and therefore is not able to assess its Y2K readiness.
AF	Congo, Democratic Republic of the	The Democratic Republic of the Congo is not heavily reliant on computerized systems, and there may be risk of potential disruption.Currently, we do not have a diplomatic presence in the Congo and, therefore, are unable to assess Y2K readiness.

Consular Information Sheets

Y2K Summaries

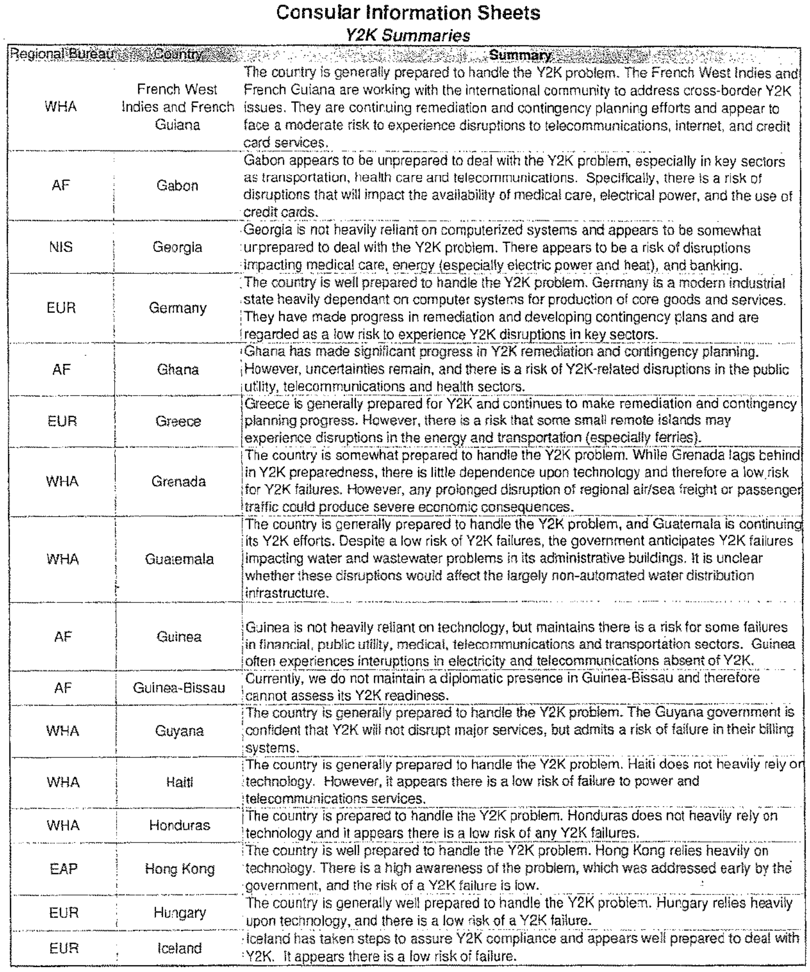
Regional Bureau	Country	Summary
AF	Congo, Republic of	The United States does not have a diplomatic presence in Comoros and therefore is not able to assess its Y2K readiness.
WHA	Costa Rica	Costa Rica appears to be generally prepared to deal with the Y2K problem. The Government of Costa Rica continues remediation efforts and contingency planning and at the present time it appears that there is a low risk of potential disruption in the key sectors.
AF	Cote d'Ivoire	Cote d'Ivoire has been modernizing many sectors of its economy and, as a result, the country is expected to experience various Y2K disruptions. As a result, serious difficulties cannot be ruled out. It appears that there is a risk of disruptions in the key sectors of electricity and fuel, banking, and telecommunications. Such disruptions may specifically affect the supply of electricity, gas and petrol, financial transfers, record keeping, and telephone services. In addition, it is likely that there will be disruptions of government services at all levels. Should these failures be prolonged, they could lead to civil disorder.
EUR	Croatia	Croatia's level of preparedness to confront the Y2K problem varies widely among crucial sectors with telecommunications and financial sectors showing the most progress. There is a risk of Y2K disruptions. However, with additional Y2K remediation efforts and contingency planning in surface transport, emergency medical services, electrical power generation, and water supply, the risk of potential disruptions will decline.
WHA	Cuba	Cuba is not heavily reliant on automated systems and is somewhat prepared to handle the Y2K problem. Although Cuba continues remediation efforts and contingency planning, at the present time it appears that there is a moderate risk of potential Y2K disruption in such key sectors as banking and finance, telecommunications, and electrical power.
EUR	Cyprus	Cyprus is generally well prepared to deal with Y2K disruptions. With increased attention to correcting Y2K problems in food storage and fuel distribution, the potential risk of disruption in Cyprus will be low by year's end. This information applies to the southern area of Cyprus under effective control of the Government of Cyprus. Little is known about Y2K compliance in the northern third of the island, and some disruptions of services can be expected.
EUR	Czech Republic	The Czech Republic appears to be generally prepared to deal with Y2K problems. There is a risk of Y2K disruptions. However, greater progress in remediation efforts and contingency planning in rail service, electricity generation, water supply and health care will help lower the risks due to Y2K.
EUR	Denmark	Denmark is a modern industrial state dependent on computer systems for a large part of its production of goods and services. It is at a low risk of Y2K disruptions in key sectors. It has made progress in remediating Y2K problems and developing contingency plans, and is well prepared to deal with the Y2K problem.
AF	Djibouti	Djibouti is not a highly automated society and travelers should not expect to encounter severe Y2K related problems. However, there are reports that telephone service could be impaired on 1/1/2000. All major hotels have generators due to already routine power outages.
WHA	Dominica	The country is somewhat prepared to handle the Y2K problem. Coordination of Y2K remediation and contingency planning has been slow in the public sector and there is a moderate risk of Y2K related disruptions in key sectors. Financial service providers and large commercial interests have been more responsive to instituting corrective measures.
WHA	Dominican Republic	The country is somewhat prepared to handle the Y2K problem. Although the Dominican Republic continues remediation efforts and contingency planning, at the present time it appears that there is a moderate risk of potential disruption in the key sectors of electrical power, water, and sanitation.



Consular Information Sheets

Y2K Summaries

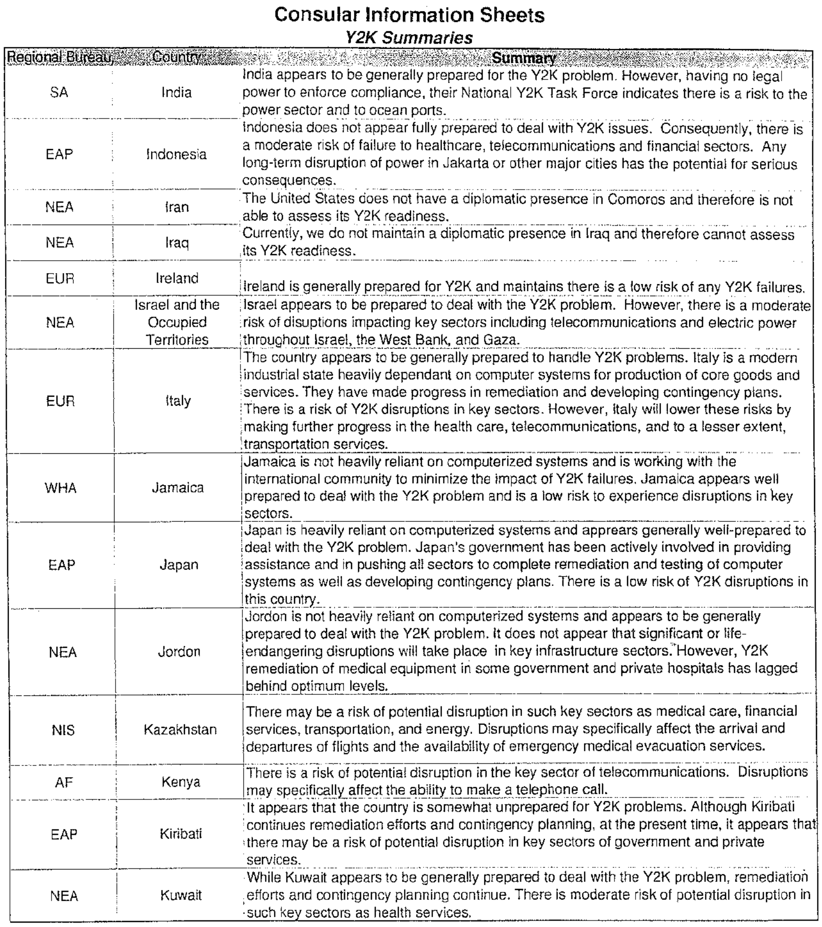
Regional Bureau	Country	Summary
WHA	Ecuador	Ecuador is not heavily reliant on computerized systems, and it appears to be somewhat prepared to deal with the Y2K problem. Although Ecuador continues remediation efforts and contingency planning, at the present time some of these remediation efforts are not complete, and it appears that there is a moderate risk of potential Y2K disruptions in key sectors, including telecommunications and energy.
NEA	Egypt	The Government of Egypt is pursuing an on-going, active Y2K program that includes remediation, testing, and contingency planning. It has made substantial progress in many areas. However, there is a risk for limited intermittent disruptions in some services including health and telecommunications.
WHA	El Salvador	The country is somewhat prepared to handle the Y2K problem, and it appears there is a moderate risk of potential Y2K disruptions in key sectors. The energy and telecommunications sectors believe their computer systems will be Y2K compliant. Hospitals and health care providers have been slower to work on compliance, and it remains to be seen how computerized medical devices will be effected.
AF	Equatorial Guinea	Currently, we do not have a diplomatic presence in the Equatorial Guinea, but the U.S. Embassy in neighboring Yaounde, Cameroon reports that there is a limited dependence on automated systems. The telecommunications system is not expected to encounter problems. Other sectors such as water, electricity, and financial systems may be particularly at risk and could be vulnerable to disruptions.
AF	Eritrea	Eritrea is not heavily reliant on computerized systems and it appears there is a low risk of potential Y2K disruptions in key sectors. Although Eritrea continues remediation efforts and contingency planning, at the present time, it appears that there may a risk of potential disruption with the interface between the domestic telephone service and international switching systems.
EUR	Estonia	Estonia had made progress in remediation and contingency planning and appears to be prepared for Y2K generated problems. Estonia's internationally-shared electric grid is a risk and is cause for concern.
AF	Ethiopia	Ethiopia regularly experiences disruptions in power, water and telecommunications services. However, many Ethiopian organizations have implemented a thorough assessment and remediation process and appears prepared for the millennium rollover.
EAP	Federated States of Micronesia	The country is generally prepared to handle the Y2K problem. In the FSM, it appears there is a low risk of potential Y2K disruptions in key sectors. The FSM is working with the international community to minimize impact on biomedical equipment, telecommunications and utilities as a result of Y2K.
EAP	Fiji	Fiji is not heavily dependant on computer systems and appears generally prepared to face the millennium. With a low risk of Y2K disruptions, key sectors are reportedly prepared and contingency plans have been developed by the Fiji Electricity Authority to address potential electrical outages.
EUR	Finland	Finland is a modern industrial state heavily dependant on computer systems and is well prepared to handle the Y2K problem. They are regarded as a low risk to experience Y2K disruptions in key sectors. Also, Finland is working with its EU member states to minimize the cross-border economic impact of Y2K problems.
EUR	Former Yugoslav Republic of Macedonia	The country is generally prepared to handle the Y2K problem. Although FYR Macedonia continues remediation efforts and contingency planning at the preset time, it appears that there may be a risk of potential disruption in the key sectors of banking and hospital care.
EUR	France and Monaco	The country is well prepared to handle the Y2K problem. France is a modern industrial state heavily dependant on computer systems for production of core goods and services. They have made progress in remediation and developing contingency plans and are regarded as a low risk to experience Y2K disruptions in key sectors.
EAP	French Polynesia	French Polynesia is not heavily dependant on computer systems and appears generally prepared to face the millennium. There is a low risk of disruption across key sectors. However, the likelihood of communications disuptions is moderate.



Consular Information Sheets

Y2K Summaries

Regional Bureau	Country	Summary
WHA	French West Indies and French Guiana	The country is generally prepared to handle the Y2K problem. The French West Indies and French Guiana are working with the international community to address cross-border Y2K issues. They are continuing remediation and contingency planning efforts and appear to face a moderate risk to experience disruptions to telecommunications, internet, and credit card services.
AF	Gabon	Gabon appears to be unprepared to deal with the Y2K problem, especially in key sectors as transportation, health care and telecommunications. Specifically, there is a risk of disruptions that will impact the availability of medical care, electrical power, and the use of credit cards.
NIS	Georgia	Georgia is not heavily reliant on computerized systems and appears to be somewhat unprepared to deal with the Y2K problem. There appears to be a risk of disruptions impacting medical care, energy (especially electric power and heat), and banking.
EUR	Germany	The country is well prepared to handle the Y2K problem. Germany is a modern industrial state heavily dependant on computer systems for production of core goods and services. They have made progress in remediation and developing contingency plans and are regarded as a low risk to experience Y2K disruptions in key sectors.
AF	Ghana	Ghana has made significant progress in Y2K remediation and contingency planning. However, uncertainties remain, and there is a risk of Y2K-related disruptions in the public utility, telecommunications and health sectors.
EUR	Greece	Greece is generally prepared for Y2K and continues to make remediation and contingency planning progress. However, there is a risk that some small remote islands may experience disruptions in the energy and transportation (especially ferries).
WHA	Grenada	The country is somewhat prepared to handle the Y2K problem. While Grenada lags behind in Y2K preparedness, there is little dependence upon technology and therefore a low risk for Y2K failures. However, any prolonged disruption of regional air/sea freight or passenger traffic could produce severe economic consequences.
WHA	Guatemala	The country is generally prepared to handle the Y2K problem, and Guatemala is continuing its Y2K efforts. Despite a low risk of Y2K failures, the government anticipates Y2K failures impacting water and wastewater problems in its administrative buildings. It is unclear whether these disruptions would affect the largely non-automated water distribution infrastructure.
AF	Guinea	Guinea is not heavily reliant on technology, but maintains there is a risk for some failures in financial, public utility, medical, telecommunications and transportation sectors. Guinea often experiences interuptions in electricity and telecommunications absent of Y2K.
AF	Guinea-Bissau	Currently, we do not maintain a diplomatic presence in Guinea-Bissau and therefore cannot assess its Y2K readiness.
WHA	Guyana	The country is generally prepared to handle the Y2K problem. The Guyana government is confident that Y2K will not disrupt major services, but admits a risk of failure in their billing systems.
WHA	Haiti	The country is generally prepared to handle the Y2K problem. Haiti does not heavily rely on technology. However, it appears there is a low risk of failure to power and telecommunications services.
WHA	Honduras	The country is prepared to handle the Y2K problem. Honduras does not heavily rely on technology and it appears there is a low risk of any Y2K failures.
EAP	Hong Kong	The country is well prepared to handle the Y2K problem. Hong Kong relies heavily on technology. There is a high awareness of the problem, which was addressed early by the government, and the risk of a Y2K failure is low.
EUR	Hungary	The country is generally well prepared to handle the Y2K problem. Hungary relies heavily upon technology, and there is a low risk of a Y2K failure.
EUR	Iceland	Iceland has taken steps to assure Y2K compliance and appears well prepared to deal with Y2K. It appears there is a low risk of failure.



Consular Information Sheets

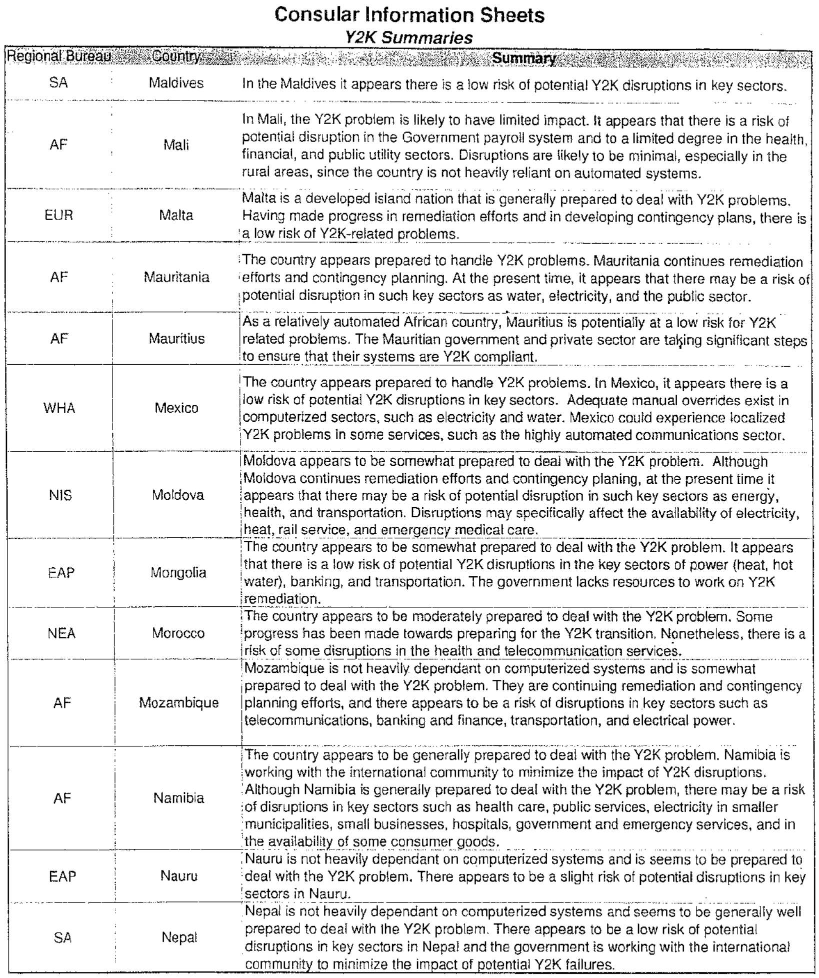
Y2K Summaries

Regional Bureau	Country	Summary
SA	India	India appears to be generally prepared for the Y2K problem. However, having no legal power to enforce compliance, their National Y2K Task Force indicates there is a risk to the power sector and to ocean ports.
EAP	Indonesia	Indonesia does not appear fully prepared to deal with Y2K issues. Consequently, there is a moderate risk of failure to healthcare, telecommunications and financial sectors. Any long-term disruption of power in Jakarta or other major cities has the potential for serious consequences.
NEA	Iran	The United States does not have a diplomatic presence in Comoros and therefore is not able to assess its Y2K readiness.
NEA	Iraq	Currently, we do not maintain a diplomatic presence in Iraq and therefore cannot assess its Y2K readiness.
EUR	Ireland	Ireland is generally prepared for Y2K and maintains there is a low risk of any Y2K failures.
NEA	Israel and the Occupied Territories	Israel appears to be prepared to deal with the Y2K problem. However, there is a moderate risk of disuptions impacting key sectors including telecommunications and electric power throughout Israel, the West Bank, and Gaza.
EUR	Italy	The country appears to be generally prepared to handle Y2K problems. Italy is a modern industrial state heavily dependant on computer systems for production of core goods and services. They have made progress in remediation and developing contingency plans. There is a risk of Y2K disruptions in key sectors. However, Italy will lower these risks by making further progress in the health care, telecommunications, and to a lesser extent, transportation services.
WHA	Jamaica	Jamaica is not heavily reliant on computerized systems and is working with the international community to minimize the impact of Y2K failures. Jamaica appears well prepared to deal with the Y2K problem and is a low risk to experience disruptions in key sectors.
EAP	Japan	Japan is heavily reliant on computerized systems and apprears generally well-prepared to deal with the Y2K problem. Japan's government has been actively involved in providing assistance and in pushing all sectors to complete remediation and testing of computer systems as well as developing contingency plans. There is a low risk of Y2K disruptions in this country.
NEA	Jordon	Jordon is not heavily reliant on computerized systems and appears to be generally prepared to deal with the Y2K problem. It does not appear that significant or life-endangering disruptions will take place in key infrastructure sectors.However, Y2K remediation of medical equipment in some government and private hospitals has lagged behind optimum levels.
NIS	Kazakhstan	There may be a risk of potential disruption in such key sectors as medical care, financial services, transportation, and energy. Disruptions may specifically affect the arrival and departures of flights and the availability of emergency medical evacuation services.
AF	Kenya	There is a risk of potential disruption in the key sector of telecommunications. Disruptions may specifically affect the ability to make a telephone call.
EAP	Kiribati	It appears that the country is somewhat unprepared for Y2K problems. Although Kiribati continues remediation efforts and contingency planning, at the present time, it appears that there may be a risk of potential disruption in key sectors of government and private services.
NEA	Kuwait	While Kuwait appears to be generally prepared to deal with the Y2K problem, remediation efforts and contingency planning continue. There is moderate risk of potential disruption in such key sectors as health services.

Consular Information Sheets

Y2K Summaries

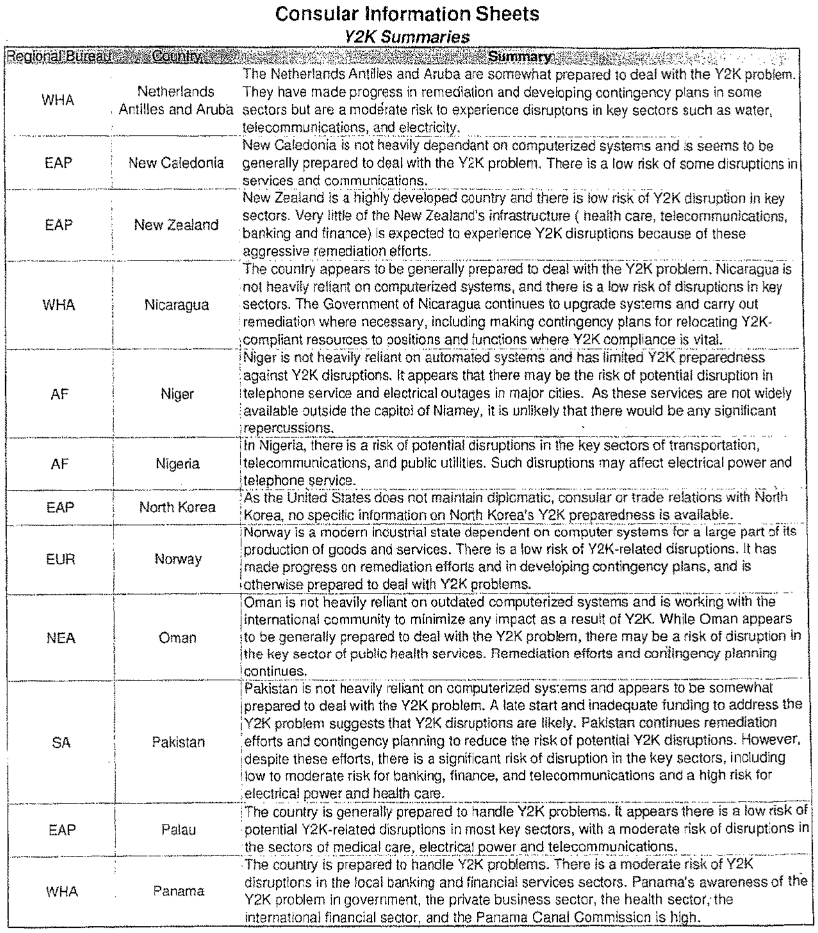
Regional Bureau	Country	Summary
NIS	Kyrgyz Republic	Although the Republic continues remediation efforts and contingency planning, at the present time, it appears that there may be a risk of potential disruption in key sectors of emergency health care and energy. Such disruptions may specifically affect the availabilty of emergency medical evaluations and exacerbate existing problems with power failure and supply.
EAP	Laos	The country appears somewhat prepared to handle Y2K problems. There may be a risk of disruption in the key sectors of energy, finance, healthcare, and telecommunications. A low probability exists for failure in the public service, transportation, and water sectors.
EUR	Latvia	The country appears generally prepared to handle Y2K problems. The country is at risk in the key sectors of electric power distribution and health care and greater progress in contingency planning is needed in order to lower these potential risks. Of particular concern is Latvia's internationally-shared electric grid.
NEA	Lebanon	The country appears generally prepared to handle Y2K problems. Although Lebanon continues some remediation efforts and contingency planning, at the present time, it appears that there may be a risk of potential disruption in key sectors of telecommunications services. However, this sector is installing new equipment and expects to be Y2K compliant by the end of the year.
AF	Lesotho	The country appears to be somewhat prepared to handle Y2K problems. Although Lesotho continues some remediation efforts and contingency planning, at the present time, it appears that there may be a risk of potential disruption in key sectors of water, electricity, health and telecommunications.
AF	Liberia	Basic services of electricity and water will not be affected by the Y2K problem. However, it appears likely that there is a risk of potential disruption in the key sector of telecommunications. Both long distance and local telephone service may be completely disrupted by the Y2K problem.
NEA	Libya	In Libya, it appears that there is a high risk of potential Y2K disruptions in key sectors, including the banking and finance sector. Information is not available to judge the scope and duration of these disruptions.
EUR	Lithuania	The country appears to be generally prepared to handle Y2K problems. There is a risk of Y2K problems in the key sector of electric power generation and distribution and greater progress in remediation efforts and contingency planning is needed in the to lower the risk of potential Y2K disruptions. Of particular concern is Lithuania's internationally-shared electric grid.
EUR	Luxembourg	Luxembourg is well prepared to deal with the possibility of the negative impact of Y2K, having made progress on remediating Y2K problems and developing contingency plans. It appears there is a low risk of potential Y2K disruptions in key sectors.
EAP	Macau	Macau is somewhat prepared to deal with the Y2K problem. Macau is less dependent on technology than many economies, and began rather late to address the Y2K issue. In general, it appears that there is a low risk of Y2K disruptions in Macau. The main area of concern is potential disruption in the medical sector.
AF	Madagascar	The Embassy has received information from the government of Madagascar indicating that potential disruptions in the water, electricity, energy, telecommunications, and banking sectors should be minimal. The U.S. Embassy cannot certify the accuracy of the Malagasy Government's assessment.
AF	Malawi	The country is somewhat prepared to handle Y2K problems. Although Malawi continues remediation efforts and contingency planning, at the present time, it appears that there may be a risk of potential disruption in such key sectors as telecommunications, electricity, water, and heath care.
EAP	Malaysia	Malaysia appears to be prepared to deal with the Y2K problem. It appears that there is a low risk of potential Y2K disruptions in the banking and finance, health, telecommunications, transportation, utilities and electric power sectors. There is also a low risk of potential Y2K disruptions at private hospitals in Malaysia.



Consular Information Sheets

Y2K Summaries

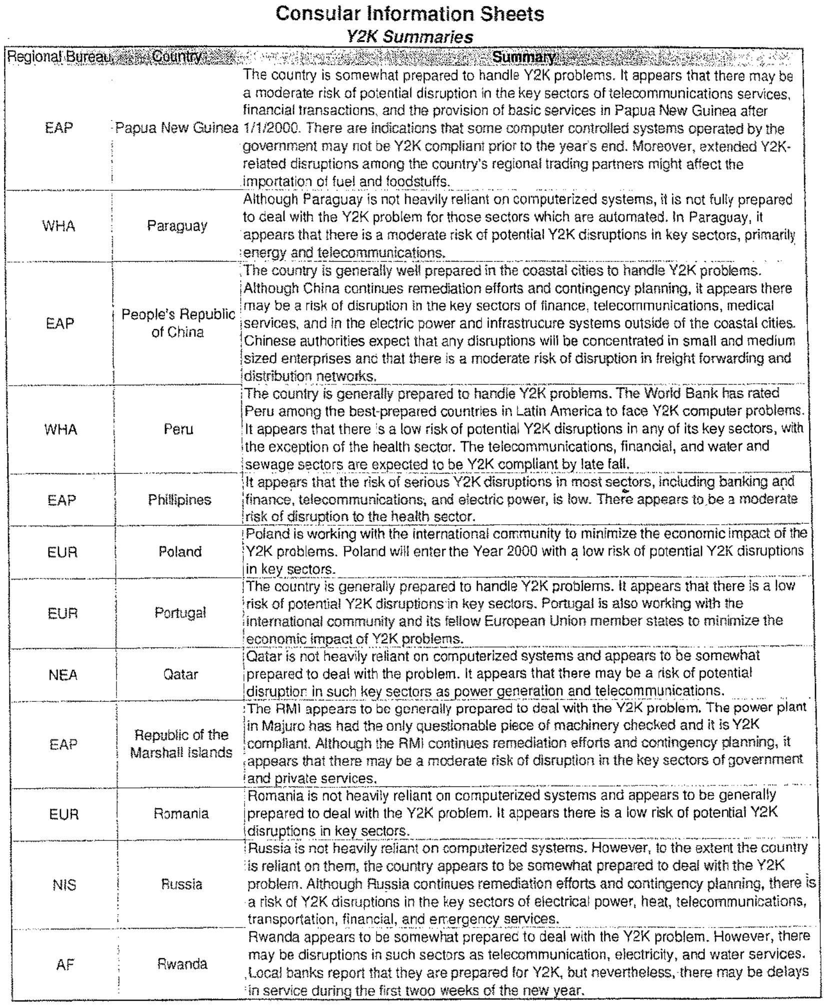
Regional Bureau	Country	Summary
SA	Maldives	In the Maldives it appears there is a low risk of potential Y2K disruptions in key sectors.
AF	Mali	In Mali, the Y2K problem is likely to have limited impact. It appears that there is a risk of potential disruption in the Government payroll system and to a limited degree in the health, financial, and public utility sectors. Disruptions are likely to be minimal, especially in the rural areas, since the country is not heavily reliant on automated systems.
EUR	Malta	Malta is a developed island nation that is generally prepared to deal with Y2K problems. Having made progress in remediation efforts and in developing contingency plans, there is a low risk of Y2K-related problems.
AF	Mauritania	The country appears prepared to handle Y2K problems. Mauritania continues remediation efforts and contingency planning. At the present time, it appears that there may be a risk of potential disruption in such key sectors as water, electricity, and the public sector.
AF	Mauritius	As a relatively automated African country, Mauritius is potentially at a low risk for Y2K related problems. The Mauritian government and private sector are taking significant steps to ensure that their systems are Y2K compliant.
WHA	Mexico	The country appears prepared to handle Y2K problems. In Mexico, it appears there is a low risk of potential Y2K disruptions in key sectors. Adequate manual overrides exist in computerized sectors, such as electricity and water. Mexico could experience localized Y2K problems in some services, such as the highly automated communications sector.
NIS	Moldova	Moldova appears to be somewhat prepared to deal with the Y2K problem. Although Moldova continues remediation efforts and contingency planing, at the present time it appears that there may be a risk of potential disruption in such key sectors as energy, health, and transportation. Disruptions may specifically affect the availability of electricity, heat, rail service, and emergency medical care.
EAP	Mongolia	The country appears to be somewhat prepared to deal with the Y2K problem. It appears that there is a low risk of potential Y2K disruptions in the key sectors of power (heat, hot water), banking, and transportation. The government lacks resources to work on Y2K remediation.
NEA	Morocco	The country appears to be moderately prepared to deal with the Y2K problem. Some progress has been made towards preparing for the Y2K transition. Nonetheless, there is a risk of some disruptions in the health and telecommunication services.
AF	Mozambique	Mozambique is not heavily dependant on computerized systems and is somewhat prepared to deal with the Y2K problem. They are continuing remediation and contingency planning efforts, and there appears to be a risk of disruptions in key sectors such as telecommunications, banking and finance, transportation, and electrical power.
AF	Namibia	The country appears to be generally prepared to deal with the Y2K problem. Namibia is working with the international community to minimize the impact of Y2K disruptions. Although Namibia is generally prepared to deal with the Y2K problem, there may be a risk of disruptions in key sectors such as health care, public services, electricity in smaller municipalities, small businesses, hospitals, government and emergency services, and in the availability of some consumer goods.
EAP	Nauru	Nauru is not heavily dependant on computerized systems and is seems to be prepared to deal with the Y2K problem. There appears to be a slight risk of potential disruptions in key sectors in Nauru.
SA	Nepal	Nepal is not heavily dependant on computerized systems and seems to be generally well prepared to deal with the Y2K problem. There appears to be a low risk of potential disruptions in key sectors in Nepal and the government is working with the international community to minimize the impact of potential Y2K failures.



Consular Information Sheets

Y2K Summaries

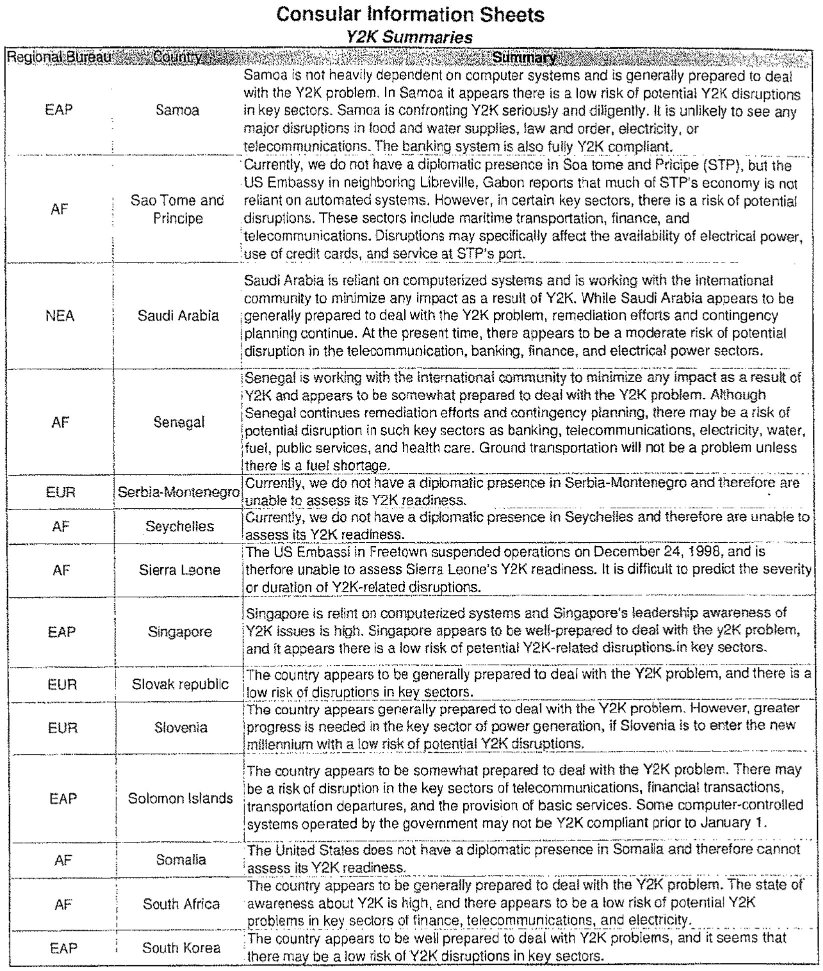
Regional Bureau	Country	Summary
WHA	Netherlands Antilles and Aruba	The Netherlands Antilles and Aruba are somewhat prepared to deal with the Y2K problem. They have made progress in remediation and developing contingency plans in some sectors but are a modérate risk to experience disruptons in key sectors such as water, telecommunications, and electricity.
EAP	New Caledonia	New Caledonia is not heavily dependant on computerized systems and is seems to be generally prepared to deal with the Y2K problem. There is a low risk of some disruptions in services and communications.
EAP	New Zealand	New Zealand is a highly developed country and there is low risk of Y2K disruption in key sectors. Very little of the New Zealand's infrastructure (health care, telecommunications, banking and finance) is expected to experience Y2K disruptions because of these aggressive remediation efforts.
WHA	Nicaragua	The country appears to be generally prepared to deal with the Y2K problem. Nicaragua is not heavily reliant on computerized systems, and there is a low risk of disruptions in key sectors. The Government of Nicaragua continues to upgrade systems and carry out remediation where necessary, including making contingency plans for relocating Y2K-compliant resources to positions and functions where Y2K compliance is vital.
AF	Niger	Niger is not heavily reliant on automated systems and has limited Y2K preparedness against Y2K disruptions. It appears that there may be the risk of potential disruption in telephone service and electrical outages in major cities. As these services are not widely available outside the capitol of Niamey, it is unlikely that there would be any significant repercussions.
AF	Nigeria	In Nigeria, there is a risk of potential disruptions in the key sectors of transportation, telecommunications, and public utilities. Such disruptions may affect electrical power and telephone service.
EAP	North Korea	As the United States does not maintain diplomatic, consular or trade relations with North Korea, no specific information on North Korea's Y2K preparedness is available.
EUR	Norway	Norway is a modern industrial state dependent on computer systems for a large part of its production of goods and services. There is a low risk of Y2K-related disruptions. It has made progress on remediation efforts and in developing contingency plans, and is otherwise prepared to deal with Y2K problems.
NEA	Oman	Oman is not heavily reliant on outdated computerized systems and is working with the international community to minimize any impact as a result of Y2K. While Oman appears to be generally prepared to deal with the Y2K problem, there may be a risk of disruption in the key sector of public health services. Remediation efforts and contingency planning continues.
SA	Pakistan	Pakistan is not heavily reliant on computerized systems and appears to be somewhat prepared to deal with the Y2K problem. A late start and inadequate funding to address the Y2K problem suggests that Y2K disruptions are likely. Pakistan continues remediation efforts and contingency planning to reduce the risk of potential Y2K disruptions. However, despite these efforts, there is a significant risk of disruption in the key sectors, including low to moderate risk for banking, finance, and telecommunications and a high risk for electrical power and health care.
EAP	Palau	The country is generally prepared to handle Y2K problems. It appears there is a low risk of potential Y2K-related disruptions in most key sectors, with a moderate risk of disruptions in the sectors of medical care, electrical power and telecommunications.
WHA	Panama	The country is prepared to handle Y2K problems. There is a moderate risk of Y2K disruptions in the local banking and financial services sectors. Panama's awareness of the Y2K problem in government, the private business sector, the health sector, the international financial sector, and the Panama Canal Commission is high.



Consular Information Sheets

Y2K Summaries

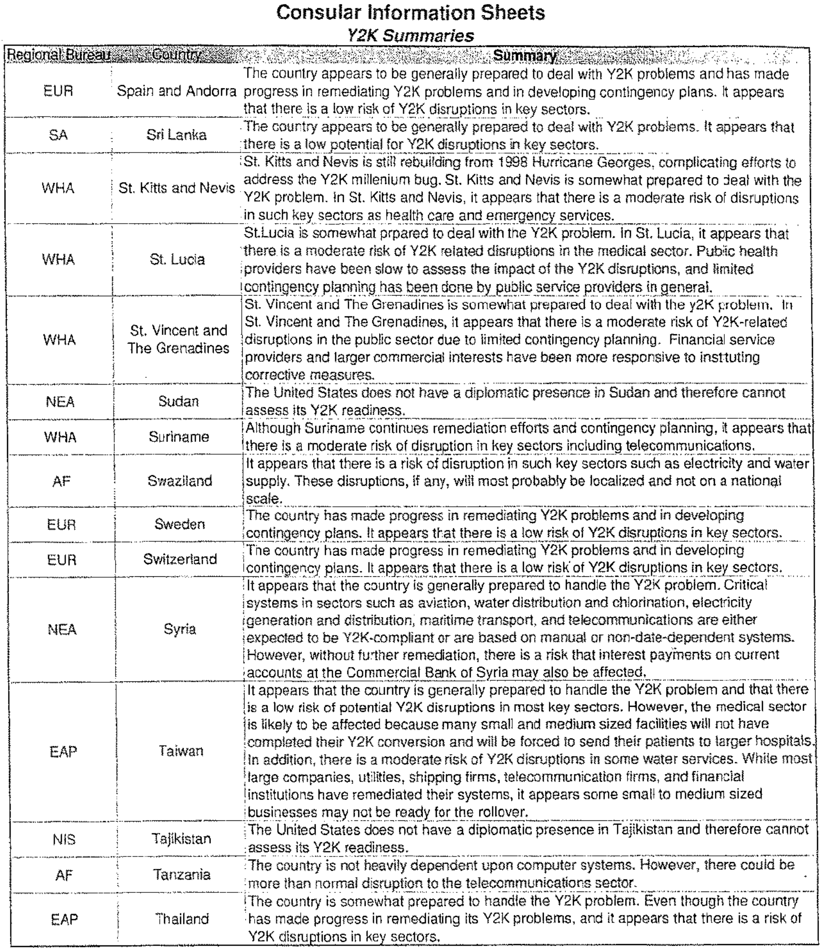
Regional Bureau	Country	Summary
EAP	Papua New Guinea	The country is somewhat prepared to handle Y2K problems. It appears that there may be a moderate risk of potential disruption in the key sectors of telecommunications services, financial transactions, and the provision of basic services in Papua New Guinea after 1/1/2000. There are indications that some computer controlled systems operated by the government may not be Y2K compliant prior to the year's end. Moreover, extended Y2K-related disruptions among the country's regional trading partners might affect the importation of fuel and foodstuffs.
WHA	Paraguay	Although Paraguay is not heavily reliant on computerized systems, it is not fully prepared to deal with the Y2K problem for those sectors which are automated. In Paraguay, it appears that there is a moderate risk of potential Y2K disruptions in key sectors, primarily energy and telecommunications.
EAP	People's Republic of China	The country is generally well prepared in the coastal cities to handle Y2K problems. Although China continues remediation efforts and contingency planning, it appears there may be a risk of disruption in the key sectors of finance, telecommunications, medical services, and in the electric power and infrastrucure systems outside of the coastal cities. Chinese authorities expect that any disruptions will be concentrated in small and medium sized enterprises and that there is a moderate risk of disruption in freight forwarding and distribution networks.
WHA	Peru	The country is generally prepared to handle Y2K problems. The World Bank has rated Peru among the best-prepared countries in Latin America to face Y2K computer problems. It appears that there is a low risk of potential Y2K disruptions in any of its key sectors, with the exception of the health sector. The telecommunications, financial, and water and sewage sectors are expected to be Y2K compliant by late fall.
EAP	Phillipines	It appears that the risk of serious Y2K disruptions in most sectors, including banking and finance, telecommunications, and electric power, is low. There appears to be a moderate risk of disruption to the health sector.
EUR	Poland	Poland is working with the international community to minimize the economic impact of the Y2K problems. Poland will enter the Year 2000 with a low risk of potential Y2K disruptions in key sectors.
EUR	Portugal	The country is generally prepared to handle Y2K problems. It appears that there is a low risk of potential Y2K disruptions in key sectors. Portugal is also working with the international community and its fellow European Union member states to minimize the economic impact of Y2K problems.
NEA	Qatar	Qatar is not heavily reliant on computerized systems and appears to be somewhat prepared to deal with the problem. It appears that there may be a risk of potential disruption in such key sectors as power generation and telecommunications.
EAP	Republic of the Marshall Islands	The RMI appears to be generally prepared to deal with the Y2K problem. The power plant in Majuro has had the only questionable piece of machinery checked and it is Y2K compliant. Although the RMI continues remediation efforts and contingency planning, it appears that there may be a moderate risk of disruption in the key sectors of government and private services.
EUR	Romania	Romania is not heavily reliant on computerized systems and appears to be generally prepared to deal with the Y2K problem. It appears there is a low risk of potential Y2K disruptions in key sectors.
NIS	Russia	Russia is not heavily reliant on computerized systems. However, to the extent the country is reliant on them, the country appears to be somewhat prepared to deal with the Y2K problem. Although Russia continues remediation efforts and contingency planning, there is a risk of Y2K disruptions in the key sectors of electrical power, heat, telecommunications, transportation, financial, and emergency services.
AF	Rwanda	Rwanda appears to be somewhat prepared to deal with the Y2K problem. However, there may be disruptions in such sectors as telecommunication, electricity, and water services. Local banks report that they are prepared for Y2K, but nevertheless, there may be delays in service during the first twoo weeks of the new year.



Consular Information Sheets

Y2K Summaries

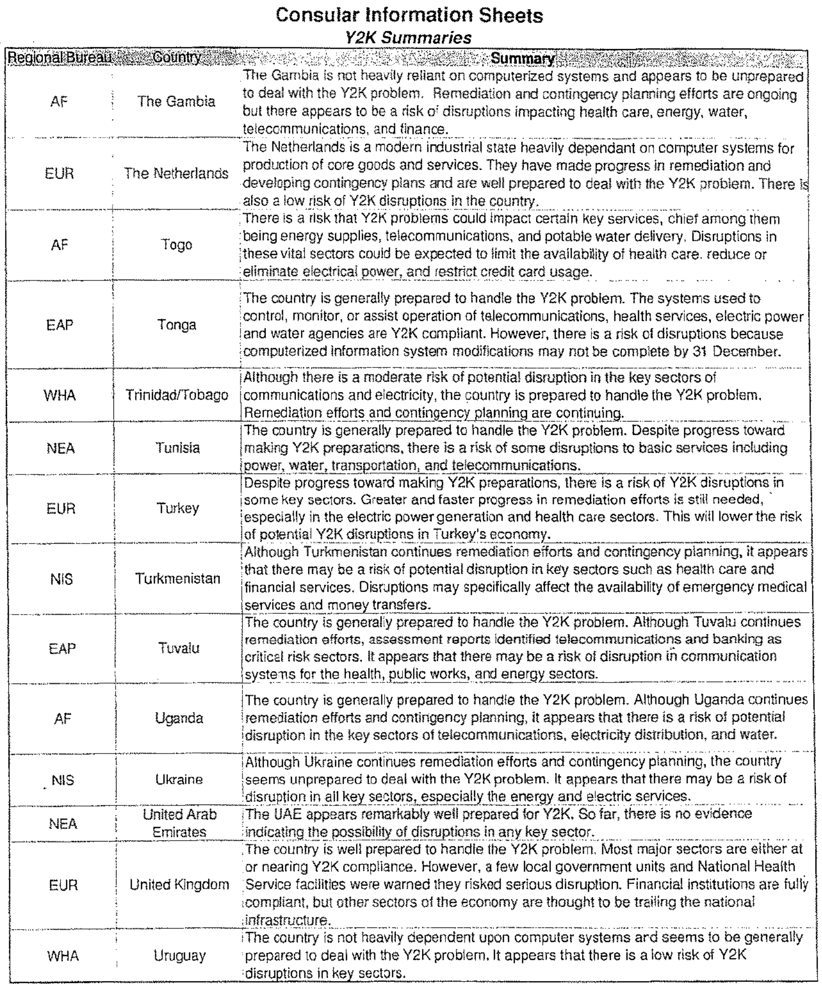
Regional Bureau	Country	Summary
EAP	Samoa	Samoa is not heavily dependent on computer systems and is generally prepared to deal with the Y2K problem. In Samoa it appears there is a low risk of potential Y2K disruptions in key sectors. Samoa is confronting Y2K seriously and diligently. It is unlikely to see any major disruptions in food and water supplies, law and order, electricity, or telecommunications. The banking system is also fully Y2K compliant.
AF	Sao Tome and Principe	Currently, we do not have a diplomatic presence in Soa tome and Pricipe (STP), but the US Embassy in neighboring Libreville, Gabon reports that much of STP's economy is not reliant on automated systems. However, in certain key sectors, there is a risk of potential disruptions. These sectors include maritime transportation, finance, and telecommunications. Disruptions may specifically affect the availability of electrical power, use of credit cards, and service at STP's port.
NEA	Saudi Arabia	Saudi Arabia is reliant on computerized systems and is working with the international community to minimize any impact as a result of Y2K. While Saudi Arabia appears to be generally prepared to deal with the Y2K problem, remediation efforts and contingency planning continue. At the present time, there appears to be a moderate risk of potential disruption in the telecommunication, banking, finance, and electrical power sectors.
AF	Senegal	Senegal is working with the international community to minimize any impact as a result of Y2K and appears to be somewhat prepared to deal with the Y2K problem. Although Senegal continues remediation efforts and contingency planning, there may be a risk of potential disruption in such key sectors as banking, telecommunications, electricity, water, fuel, public services, and health care. Ground transportation will not be a problem unless there is a fuel shortage.
EUR	Serbia-Montenegro	Currently, we do not have a diplomatic presence in Serbia-Montenegro and therefore are unable to assess its Y2K readiness.
AF	Seychelles	Currently, we do not have a diplomatic presence in Seychelles and therefore are unable to assess its Y2K readiness.
AF	Sierra Leone	The US Embassi in Freetown suspended operations on December 24, 1998, and is therfore unable to assess Sierra Leone's Y2K readiness. It is difficult to predict the severity or duration of Y2K-related disruptions.
EAP	Singapore	Singapore is relint on computerized systems and Singapore's leadership awareness of Y2K issues is high. Singapore appears to be well-prepared to deal with the y2K problem, and it appears there is a low risk of petential Y2K-related disruptions.in key sectors.
EUR	Slovak republic	The country appears to be generally prepared to deal with the Y2K problem, and there is a low risk of disruptions in key sectors.
EUR	Slovenia	The country appears generally prepared to deal with the Y2K problem. However, greater progress is needed in the key sector of power generation, if Slovenia is to enter the new millennium with a low risk of potential Y2K disruptions.
EAP	Solomon Islands	The country appears to be somewhat prepared to deal with the Y2K problem. There may be a risk of disruption in the key sectors of telecommunications, financial transactions, transportation departures, and the provision of basic services. Some computer-controlled systems operated by the government may not be Y2K compliant prior to January 1.
AF	Somalia	The United States does not have a diplomatic presence in Somalia and therefore cannot assess its Y2K readiness.
AF	South Africa	The country appears to be generally prepared to deal with the Y2K problem. The state of awareness about Y2K is high, and there appears to be a low risk of potential Y2K problems in key sectors of finance, telecommunications, and electricity.
EAP	South Korea	The country appears to be well prepared to deal with Y2K problems, and it seems that there may be a low risk of Y2K disruptions in key sectors.



Consular Information Sheets

Y2K Summaries

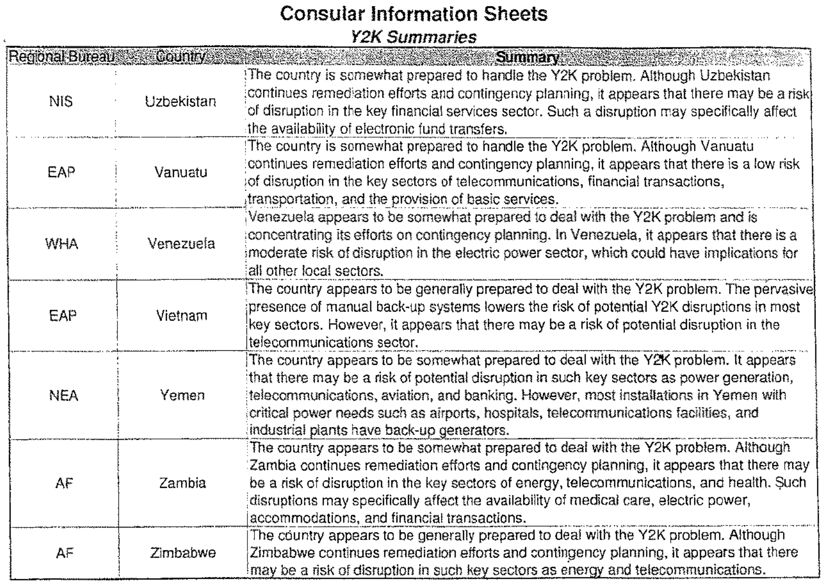
Regional Bureau	Country	Summary
EUR	Spain and Andorra	The country appears to be generally prepared to deal with Y2K problems and has made progress in remediating Y2K problems and in developing contingency plans. It appears that there is a low risk of Y2K disruptions in key sectors.
SA	Sri Lanka	The country appears to be generally prepared to deal with Y2K problems. It appears that there is a low potential for Y2K disruptions in key sectors.
WHA	St. Kitts and Nevis	St. Kitts and Nevis is still rebuilding from 1998 Hurricane Georges, complicating efforts to address the Y2K millenium bug. St. Kitts and Nevis is somewhat prepared to deal with the Y2K problem. In St. Kitts and Nevis, it appears that there is a moderate risk of disruptions in such key sectors as health care and emergency services.
WHA	St. Lucia	St.Lucia is somewhat prpared to deal with the Y2K problem. In St. Lucia, it appears that there is a moderate risk of Y2K related disruptions in the medical sector. Public health providers have been slow to assess the impact of the Y2K disruptions, and limited contingency planning has been done by public service providers in general.
WHA	St. Vincent and The Grenadines	St. Vincent and The Grenadines is somewhat prepared to deal with the y2K problem. In St. Vincent and The Grenadines, it appears that there is a moderate risk of Y2K-related disruptions in the public sector due to limited contingency planning. Financial service providers and larger commercial interests have been more responsive to insttuting corrective measures.
NEA	Sudan	The United States does not have a diplomatic presence in Sudan and therefore cannot assess its Y2K readiness.
WHA	Suriname	Although Suriname continues remediation efforts and contingency planning, it appears that there is a moderate risk of disruption in key sectors including telecommunications.
AF	Swaziland	It appears that there is a risk of disruption in such key sectors such as electricity and water supply. These disruptions, if any, will most probably be localized and not on a national scale.
EUR	Sweden	The country has made progress in remediating Y2K problems and in developing contingency plans. It appears that there is a low risk of Y2K disruptions in key sectors.
EUR	Switzerland	The country has made progress in remediating Y2K problems and in developing contingency plans. It appears that there is a low risk of Y2K disruptions in key sectors.
NEA	Syria	It appears that the country is generally prepared to handle the Y2K problem. Critical systems in sectors such as aviation, water distribution and chlorination, electricity generation and distribution, maritime transport, and telecommunications are either expected to be Y2K-compliant or are based on manual or non-date-dependent systems. However, without further remediation, there is a risk that interest payments on current accounts at the Commercial Bank of Syria may also be affected.
EAP	Taiwan	It appears that the country is generally prepared to handle the Y2K problem and that there is a low risk of potential Y2K disruptions in most key sectors. However, the medical sector is likely to be affected because many small and medium sized facilities will not have completed their Y2K conversion and will be forced to send their patients to larger hospitals. In addition, there is a moderate risk of Y2K disruptions in some water services. While most large companies, utilities, shipping firms, telecommunication firms, and financial institutions have remediated their systems, it appears some small to medium sized businesses may not be ready for the rollover.
NIS	Tajikistan	The United States does not have a diplomatic presence in Tajikistan and therefore cannot assess its Y2K readiness.
AF	Tanzania	The country is not heavily dependent upon computer systems. However, there could be more than normal disruption to the telecommunications sector.
EAP	Thailand	The country is somewhat prepared to handle the Y2K problem. Even though the country has made progress in remediating its Y2K problems, and it appears that there is a risk of Y2K disruptions in key sectors.



Consular Information Sheets

Y2K Summaries

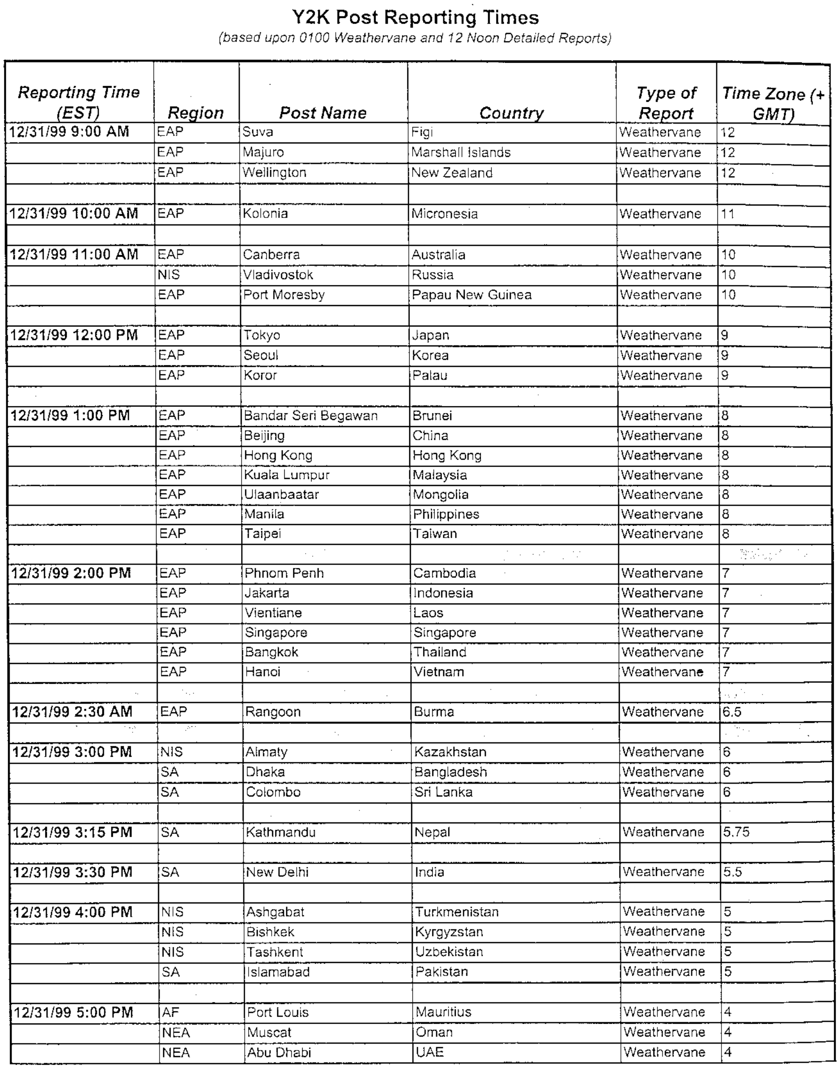
Regional Bureau	Country	Summary
AF	The Gambia	The Gambia is not heavily reliant on computerized systems and appears to be unprepared to deal with the Y2K problem. Remediation and contingency planning efforts are ongoing but there appears to be a risk o' disruptions impacting health care, energy, water, telecommunications, and finance.
EUR	The Netherlands	The Netherlands is a modern industrial state heavily dependant on computer systems for production of core goods and services. They have made progress in remediation and developing contingency plans and are well prepared to deal with the Y2K problem. There is also a low risk of Y2K disruptions in the country.
AF	Togo	There is a risk that Y2K problems could impact certain key services, chief among them being energy supplies, telecommunications, and potable water delivery. Disruptions in these vital sectors could be expected to limit the availability of health care. reduce or eliminate electrical power, and restrict credit card usage.
EAP	Tonga	The country is generally prepared to handle the Y2K problem. The systems used to control, monitor, or assist operation of telecommunications, health services, electric power and water agencies are Y2K compliant. However, there is a risk of disruptions because computerized information system modifications may not be complete by 31 December.
WHA	Trinidad/Tobago	Although there is a moderate risk of potential disruption in the key sectors of communications and electricity, the country is prepared to handle the Y2K problem. Remediation efforts and contingency planning are continuing.
NEA	Tunisia	The country is generally prepared to handle the Y2K problem. Despite progress toward making Y2K preparations, there is a risk of some disruptions to basic services including power, water, transportation, and telecommunications.
EUR	Turkey	Despite progress toward making Y2K preparations, there is a risk of Y2K disruptions in some key sectors. Greater and faster progress in remediation efforts is still needed, especially in the electric power generation and health care sectors. This will lower the risk of potential Y2K disruptions in Turkey's economy.
NIS	Turkmenistan	Although Turkmenistan continues remediation efforts and contingency planning, it appears that there may be a risk of potential disruption in key sectors such as health care and financial services. Disruptions may specifically affect the availability of emergency medical services and money transfers.
EAP	Tuvalu	The country is generally prepared to handle the Y2K problem. Although Tuvalu continues remediation efforts, assessment reports identified telecommunications and banking as critical risk sectors. It appears that there may be a risk of disruption in communication systems for the health, public works, and energy sectors.
AF	Uganda	The country is generally prepared to handle the Y2K problem. Although Uganda continues remediation efforts and contingency planning, it appears that there is a risk of potential disruption in the key sectors of telecommunications, electricity distribution, and water.
NIS	Ukraine	Although Ukraine continues remediation efforts and contingency planning, the country seems unprepared to deal with the Y2K problem. It appears that there may be a risk of disruption in all key sectors, especially the energy and electric services.
NEA	United Arab Emirates	The UAE appears remarkably well prepared for Y2K. So far, there is no evidence indicating the possibility of disruptions in any key sector.
EUR	United Kingdom	The country is well prepared to handle the Y2K problem. Most major sectors are either at or nearing Y2K compliance. However, a few local government units and National Health Service facilities were warned they risked serious disruption. Financial institutions are fully compliant, but other sectors of the economy are thought to be trailing the national infrastructure.
WHA	Uruguay	The country is not heavily dependent upon computer systems and seems to be generally prepared to deal with the Y2K problem. It appears that there is a low risk of Y2K disruptions in key sectors.



Consular Information Sheets

Y2K Summaries

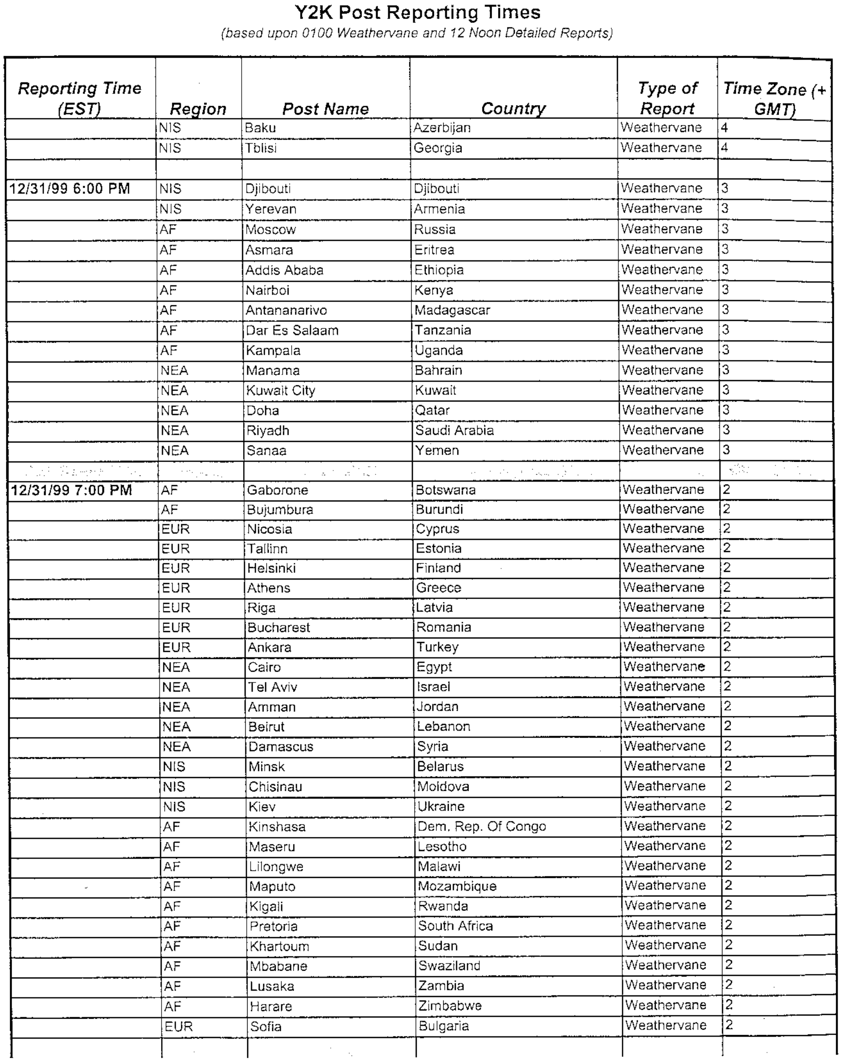
Regional Bureau	Country	Summary
NIS	Uzbekistan	The country is somewhat prepared to handle the Y2K problem. Although Uzbekistan continues remediation efforts and contingency planning, it appears that there may be a risk of disruption in the key financial services sector. Such a disruption may specifically affect the availability of electronic fund transfers.
EAP	Vanuatu	The country is somewhat prepared to handle the Y2K problem. Although Vanuatu continues remediation efforts and contingency planning, it appears that there is a low risk of disruption in the key sectors of telecommunications, financial transactions, transportation, and the provision of basic services.
WHA	Venezuela	Venezuela appears to be somewhat prepared to deal with the Y2K problem and is concentrating its efforts on contingency planning. In Venezuela, it appears that there is a moderate risk of disruption in the electric power sector, which could have implications for all other local sectors.
EAP	Vietnam	The country appears to be generally prepared to deal with the Y2K problem. The pervasive presence of manual back-up systems lowers the risk of potential Y2K disruptions in most key sectors. However, it appears that there may be a risk of potential disruption in the telecommunications sector.
NEA	Yemen	The country appears to be somewhat prepared to deal with the Y2K problem. It appears that there may be a risk of potential disruption in such key sectors as power generation, telecommunications, aviation, and banking. However, most installations in Yemen with critical power needs such as airports, hospitals, telecommunications facilities, and industrial plants have back-up generators.
AF	Zambia	The country appears to be somewhat prepared to deal with the Y2K problem. Although Zambia continues remediation efforts and contingency planning, it appears that there may be a risk of disruption in the key sectors of energy, telecommunications, and health. Such disruptions may specifically affect the availability of medical care, electric power, accommodations, and financial transactions.
AF	Zimbabwe	The country appears to be generally prepared to deal with the Y2K problem. Although Zimbabwe continues remediation efforts and contingency planning, it appears that there may be a risk of disruption in such key sectors as energy and telecommunications.



Y2K Post Reporting Times

(based upon 0100 Weathervane and 12 Noon Detailed Reports)

Reporting Time (EST)	*Region*	*Post Name*	*Country*	*Type of Report*	*Time Zone (+ GMT)*
12/31/99 9:00 AM	EAP	Suva	Figi	Weathervane	12
	EAP	Majuro	Marshall Islands	Weathervane	12
	EAP	Wellington	New Zealand	Weathervane	12
12/31/99 10:00 AM	EAP	Kolonia	Micronesia	Weathervane	11
12/31/99 11:00 AM	EAP	Canberra	Australia	Weathervane	10
	NIS	Vladivostok	Russia	Weathervane	10
	EAP	Port Moresby	Papau New Guinea	Weathervane	10
12/31/99 12:00 PM	EAP	Tokyo	Japan	Weathervane	9
	EAP	Seoul	Korea	Weathervane	9
	EAP	Koror	Palau	Weathervane	9
12/31/99 1:00 PM	EAP	Bandar Seri Begawan	Brunei	Weathervane	8
	EAP	Beijing	China	Weathervane	8
	EAP	Hong Kong	Hong Kong	Weathervane	8
	EAP	Kuala Lumpur	Malaysia	Weathervane	8
	EAP	Ulaanbaatar	Mongolia	Weathervane	8
	EAP	Manila	Philippines	Weathervane	8
	EAP	Taipei	Taiwan	Weathervane	8
12/31/99 2:00 PM	EAP	Phnom Penh	Cambodia	Weathervane	7
	EAP	Jakarta	Indonesia	Weathervane	7
	EAP	Vientiane	Laos	Weathervane	7
	EAP	Singapore	Singapore	Weathervane	7
	EAP	Bangkok	Thailand	Weathervane	7
	EAP	Hanoi	Vietnam	Weathervane	7
12/31/99 2:30 AM	EAP	Rangoon	Burma	Weathervane	6.5
12/31/99 3:00 PM	NIS	Almaty	Kazakhstan	Weathervane	6
	SA	Dhaka	Bangladesh	Weathervane	6
	SA	Colombo	Sri Lanka	Weathervane	6
12/31/99 3:15 PM	SA	Kathmandu	Nepal	Weathervane	5.75
12/31/99 3:30 PM	SA	New Delhi	India	Weathervane	5.5
12/31/99 4:00 PM	NIS	Ashgabat	Turkmenistan	Weathervane	5
	NIS	Bishkek	Kyrgyzstan	Weathervane	5
	NIS	Tashkent	Uzbekistan	Weathervane	5
	SA	Islamabad	Pakistan	Weathervane	5
12/31/99 5:00 PM	AF	Port Louis	Mauritius	Weathervane	4
	NEA	Muscat	Oman	Weathervane	4
	NEA	Abu Dhabi	UAE	Weathervane	4



Y2K Post Reporting Times

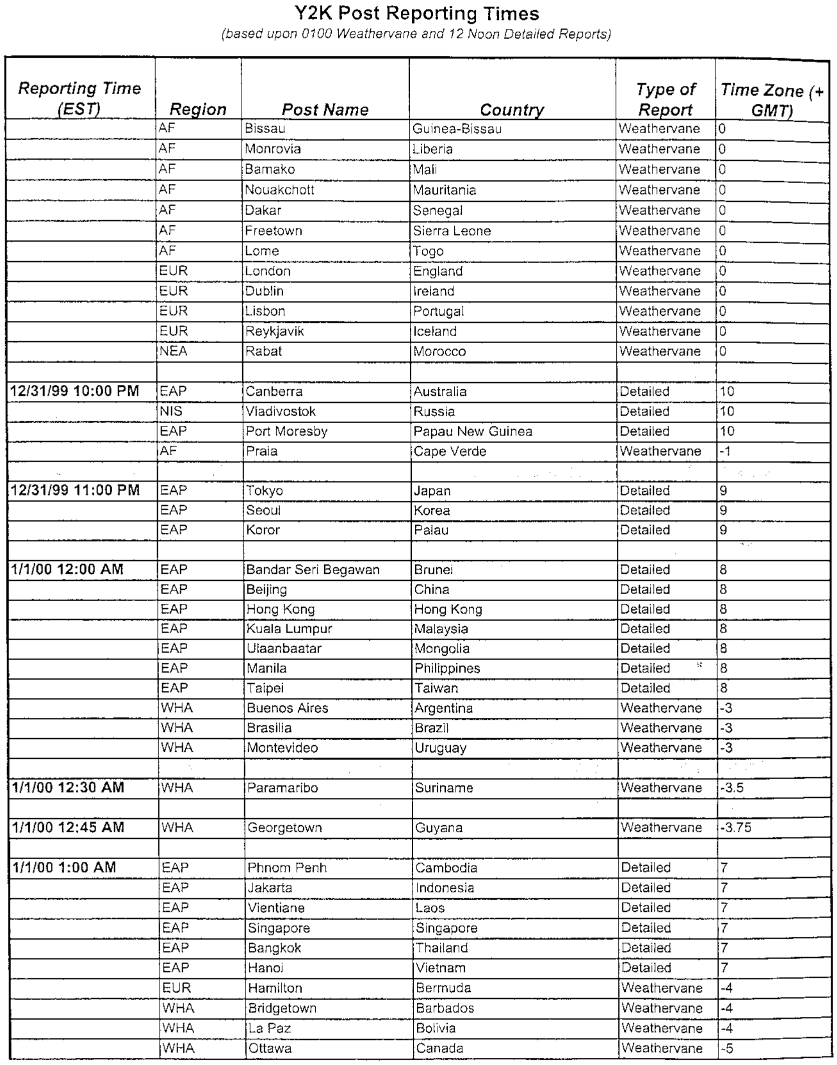
(based upon 0100 Weathervane and 12 Noon Detailed Reports)

Reporting Time (EST)	*Region*	*Post Name*	*Country*	*Type of Report*	*Time Zone (+ GMT)*
	NIS	Baku	Azerbijan	Weathervane	4
	NIS	Tblisi	Georgia	Weathervane	4
12/31/99 6:00 PM	NIS	Djibouti	Djibouti	Weathervane	3
	NIS	Yerevan	Armenia	Weathervane	3
	AF	Moscow	Russia	Weathervane	3
	AF	Asmara	Eritrea	Weathervane	3
	AF	Addis Ababa	Ethiopia	Weathervane	3
	AF	Nairboi	Kenya	Weathervane	3
	AF	Antananarivo	Madagascar	Weathervane	3
	AF	Dar Es Salaam	Tanzania	Weathervane	3
	AF	Kampala	Uganda	Weathervane	3
	NEA	Manama	Bahrain	Weathervane	3
	NEA	Kuwait City	Kuwait	Weathervane	3
	NEA	Doha	Qatar	Weathervane	3
	NEA	Riyadh	Saudi Arabia	Weathervane	3
	NEA	Sanaa	Yemen	Weathervane	3
12/31/99 7:00 PM	AF	Gaborone	Botswana	Weathervane	2
	AF	Bujumbura	Burundi	Weathervane	2
	EUR	Nicosia	Cyprus	Weathervane	2
	EUR	Tallinn	Estonia	Weathervane	2
	EUR	Helsinki	Finland	Weathervane	2
	EUR	Athens	Greece	Weathervane	2
	EUR	Riga	Latvia	Weathervane	2
	EUR	Bucharest	Romania	Weathervane	2
	EUR	Ankara	Turkey	Weathervane	2
	NEA	Cairo	Egypt	Weathervane	2
	NEA	Tel Aviv	Israel	Weathervane	2
	NEA	Amman	Jordan	Weathervane	2
	NEA	Beirut	Lebanon	Weathervane	2
	NEA	Damascus	Syria	Weathervane	2
	NIS	Minsk	Belarus	Weathervane	2
	NIS	Chisinau	Moldova	Weathervane	2
	NIS	Kiev	Ukraine	Weathervane	2
	AF	Kinshasa	Dem. Rep. Of Congo	Weathervane	2
	AF	Maseru	Lesotho	Weathervane	2
	AF	Lilongwe	Malawi	Weathervane	2
	AF	Maputo	Mozambique	Weathervane	2
	AF	Kigali	Rwanda	Weathervane	2
	AF	Pretoria	South Africa	Weathervane	2
	AF	Khartoum	Sudan	Weathervane	2
	AF	Mbabane	Swaziland	Weathervane	2
	AF	Lusaka	Zambia	Weathervane	2
	AF	Harare	Zimbabwe	Weathervane	2
	EUR	Sofia	Bulgaria	Weathervane	2

Y2K Post Reporting Times

(based upon 0100 Weathervane and 12 Noon Detailed Reports)

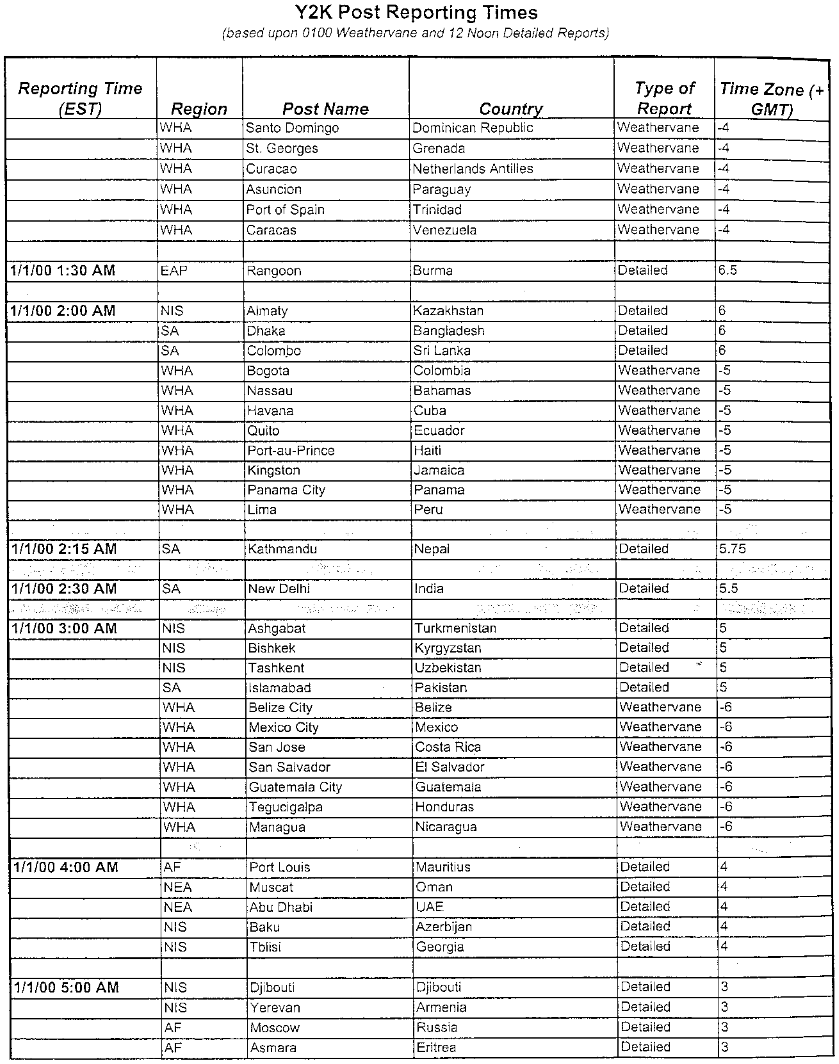
Reporting Time (EST)	*Region*	*Post Name*	*Country*	*Type of Report*	*Time Zone (+ GMT)*
12/31/99 8:00 PM	EAP	Suva	Figi	Detailed	12
	EAP	Majuro	Marshall Islands	Detailed	12
	EAP	Wellington	New Zealand	Detailed	12
	AF	Luanda	Angola	Weathervane	1
	AF	Cotonou	Benin	Weathervane	1
	AF	Yaounde	Cameroon	Weathervane	1
	AF	Bangui	Central AF Rep	Weathervane	1
	AF	N'Djamena	Chad	Weathervane	1
	AF	Brazzaville	Congo	Weathervane	1
	AF	Libreville	Gabon	Weathervane	1
	AF	Windhoek	Namibia	Weathervane	1
	AF	Lagos	Nigeria	Weathervane	1
	EUR	Zagreb	Croatia	Weathervane	1
	EUR	Prague	Czech Republic	Weathervane	1
	EUR	Copenhagen	Denmark	Weathervane	1
	EUR	Paris	France	Weathervane	1
	EUR	Berlin	Germany	Weathervane	1
	EUR	Budapest	Hungary	Weathervane	1
	EUR	Rome	Italy	Weathervane	1
	EUR	Vilnius	Lithuania	Weathervane	1
	EUR	Luxembourg	Luxembourg	Weathervane	1
	EUR	Skopje	Macedonia	Weathervane	1
	EUR	Valletta	Malta	Weathervane	1
	EUR	Oslo	Norway	Weathervane	1
	EUR	Warsaw	Poland	Weathervane	1
	EUR	Belgrade	Serbia	Weathervane	1
	EUR	Bratislava	Slovakia	Weathervane	1
	EUR	Ljubiana	Slovenia	Weathervane	1
	EUR	Madrid	Spain	Weathervane	1
	EUR	Stockholm	Sweden	Weathervane	1
	EUR	Bern	Switzerland	Weathervane	1
	EUR	The Hague	The Netherlands	Weathervane	1
	EUR	Holy See	The Vatican	Weathervane	1
	EUR	Tirana	Albania	Weathervane	1
	EUR	Vienna	Austria	Weathervane	1
	EUR	Brussels	Belgium	Weathervane	1
	EUR	Sarajevo	Bosnia Herzegovina	Weathervane	1
	AF	Niamey	Niger	Weathervane	1
	NEA	Algiers	Algeria	Weathervane	1
	NEA	Tunis	Tunisia	Weathervane	1
12/31/99 9:00 PM	EAP	Kolonia	Micronesia	Detailed	11
	AF	Ouagadougou	Burkina Faso	Weathervane	0
	AF	Abidjan	Cote d'Ivoire	Weathervane	0
	AF	BanJul	Gambia	Weathervane	0
	AF	Accra	Ghana	Weathervane	0
	AF	Conakry	Guinea	Weathervane	0



Y2K Post Reporting Times

(based upon 0100 Weathervane and 12 Noon Detailed Reports)

Reporting Time (EST)	*Region*	*Post Name*	*Country*	*Type of Report*	*Time Zone (+ GMT)*
	AF	Bissau	Guinea-Bissau	Weathervane	0
	AF	Monrovia	Liberia	Weathervane	0
	AF	Bamako	Mali	Weathervane	0
	AF	Nouakchott	Mauritania	Weathervane	0
	AF	Dakar	Senegal	Weathervane	0
	AF	Freetown	Sierra Leone	Weathervane	0
	AF	Lome	Togo	Weathervane	0
	EUR	London	England	Weathervane	0
	EUR	Dublin	Ireland	Weathervane	0
	EUR	Lisbon	Portugal	Weathervane	0
	EUR	Reykjavik	Iceland	Weathervane	0
	NEA	Rabat	Morocco	Weathervane	0
12/31/99 10:00 PM	EAP	Canberra	Australia	Detailed	10
	NIS	Vladivostok	Russia	Detailed	10
	EAP	Port Moresby	Papau New Guinea	Detailed	10
	AF	Praia	Cape Verde	Weathervane	-1
12/31/99 11:00 PM	EAP	Tokyo	Japan	Detailed	9
	EAP	Seoul	Korea	Detailed	9
	EAP	Koror	Palau	Detailed	9
1/1/00 12:00 AM	EAP	Bandar Seri Begawan	Brunei	Detailed	8
	EAP	Beijing	China	Detailed	8
	EAP	Hong Kong	Hong Kong	Detailed	8
	EAP	Kuala Lumpur	Malaysia	Detailed	8
	EAP	Ulaanbaatar	Mongolia	Detailed	8
	EAP	Manila	Philippines	Detailed	8
	EAP	Taipei	Taiwan	Detailed	8
	WHA	Buenos Aires	Argentina	Weathervane	-3
	WHA	Brasilia	Brazil	Weathervane	-3
	WHA	Montevideo	Uruguay	Weathervane	-3
1/1/00 12:30 AM	WHA	Paramaribo	Suriname	Weathervane	-3.5
1/1/00 12:45 AM	WHA	Georgetown	Guyana	Weathervane	-3.75
1/1/00 1:00 AM	EAP	Phnom Penh	Cambodia	Detailed	7
	EAP	Jakarta	Indonesia	Detailed	7
	EAP	Vientiane	Laos	Detailed	7
	EAP	Singapore	Singapore	Detailed	7
	EAP	Bangkok	Thailand	Detailed	7
	EAP	Hanoi	Vietnam	Detailed	7
	EUR	Hamilton	Bermuda	Weathervane	-4
	WHA	Bridgetown	Barbados	Weathervane	-4
	WHA	La Paz	Bolivia	Weathervane	-4
	WHA	Ottawa	Canada	Weathervane	-5



Y2K Post Reporting Times

(based upon 0100 Weathervane and 12 Noon Detailed Reports)

Reporting Time (EST)	*Region*	*Post Name*	*Country*	*Type of Report*	*Time Zone (+ GMT)*
	WHA	Santo Domingo	Dominican Republic	Weathervane	-4
	WHA	St. Georges	Grenada	Weathervane	-4
	WHA	Curacao	Netherlands Antilles	Weathervane	-4
	WHA	Asuncion	Paraguay	Weathervane	-4
	WHA	Port of Spain	Trinidad	Weathervane	-4
	WHA	Caracas	Venezuela	Weathervane	-4
1/1/00 1:30 AM	EAP	Rangoon	Burma	Detailed	6.5
1/1/00 2:00 AM	NIS	Almaty	Kazakhstan	Detailed	6
	SA	Dhaka	Bangladesh	Detailed	6
	SA	Colombo	Sri Lanka	Detailed	6
	WHA	Bogota	Colombia	Weathervane	-5
	WHA	Nassau	Bahamas	Weathervane	-5
	WHA	Havana	Cuba	Weathervane	-5
	WHA	Quito	Ecuador	Weathervane	-5
	WHA	Port-au-Prince	Haiti	Weathervane	-5
	WHA	Kingston	Jamaica	Weathervane	-5
	WHA	Panama City	Panama	Weathervane	-5
	WHA	Lima	Peru	Weathervane	-5
1/1/00 2:15 AM	SA	Kathmandu	Nepal	Detailed	5.75
1/1/00 2:30 AM	SA	New Delhi	India	Detailed	5.5
1/1/00 3:00 AM	NIS	Ashgabat	Turkmenistan	Detailed	5
	NIS	Bishkek	Kyrgyzstan	Detailed	5
	NIS	Tashkent	Uzbekistan	Detailed	5
	SA	Islamabad	Pakistan	Detailed	5
	WHA	Belize City	Belize	Weathervane	-6
	WHA	Mexico City	Mexico	Weathervane	-6
	WHA	San Jose	Costa Rica	Weathervane	-6
	WHA	San Salvador	El Salvador	Weathervane	-6
	WHA	Guatemala City	Guatemala	Weathervane	-6
	WHA	Tegucigalpa	Honduras	Weathervane	-6
	WHA	Managua	Nicaragua	Weathervane	-6
1/1/00 4:00 AM	AF	Port Louis	Mauritius	Detailed	4
	NEA	Muscat	Oman	Detailed	4
	NEA	Abu Dhabi	UAE	Detailed	4
	NIS	Baku	Azerbijan	Detailed	4
	NIS	Tbilisi	Georgia	Detailed	4
1/1/00 5:00 AM	NIS	Djibouti	Djibouti	Detailed	3
	NIS	Yerevan	Armenia	Detailed	3
	AF	Moscow	Russia	Detailed	3
	AF	Asmara	Eritrea	Detailed	3

Y2K Post Reporting Times

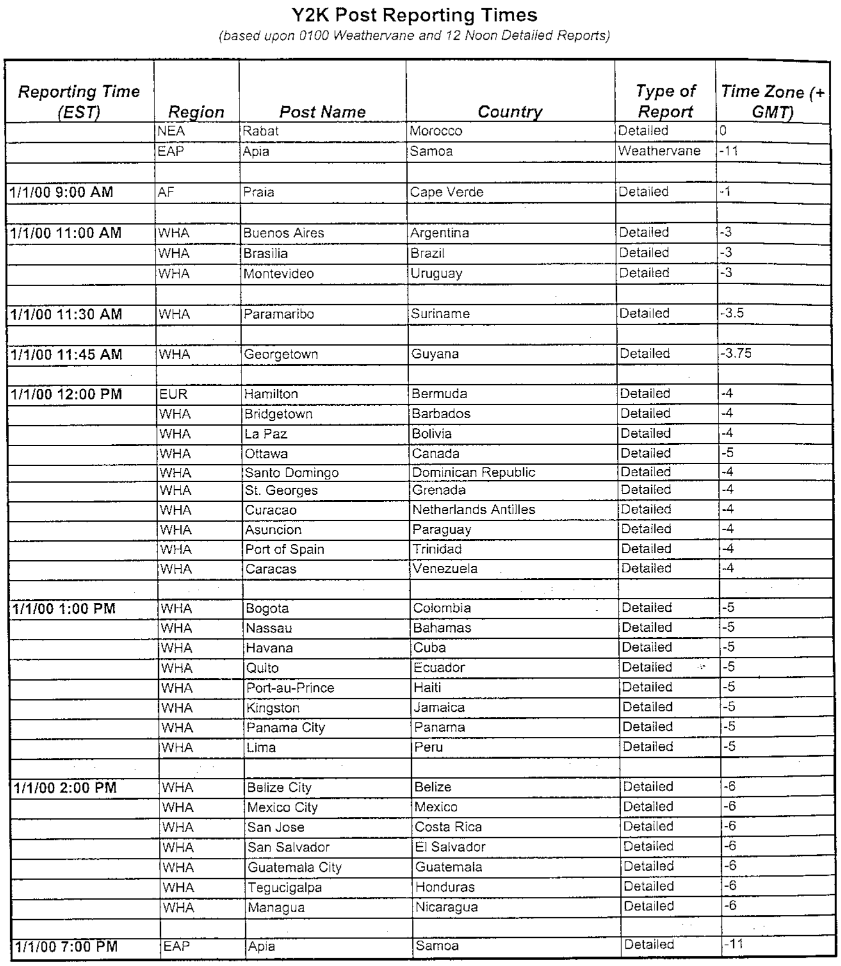
(based upon 0100 Weathervane and 12 Noon Detailed Reports)

Reporting Time (EST)	*Region*	*Post Name*	*Country*	*Type of Report*	*Time Zone (+ GMT)*
	AF	Addis Ababa	Ethiopia	Detailed	3
	AF	Nairboi	Kenya	Detailed	3
	AF	Antananarivo	Madagascar	Detailed	3
	AF	Dar Es Salaam	Tanzania	Detailed	3
	AF	Kampala	Uganda	Detailed	3
	NEA	Manama	Bahrain	Detailed	3
	NEA	Kuwait City	Kuwait	Detailed	3
	NEA	Doha	Qatar	Detailed	3
	NEA	Riyadh	Saudi Arabia	Detailed	3
	NEA	Sanaa	Yemen	Detailed	3
1/1/00 6:00 AM	AF	Gaborone	Botswana	Detailed	2
	AF	Bujumbura	Burundi	Detailed	2
	EUR	Nicosia	Cyprus	Detailed	2
	EUR	Tallinn	Estonia	Detailed	2
	EUR	Helsinki	Finland	Detailed	2
	EUR	Athens	Greece	Detailed	2
	EUR	Riga	Latvia	Detailed	2
	EUR	Bucharest	Romania	Detailed	2
	EUR	Ankara	Turkey	Detailed	2
	NEA	Cairo	Egypt	Detailed	2
	NEA	Tel Aviv	Israel	Detailed	2
	NEA	Amman	Jordan	Detailed	2
	NEA	Beirut	Lebanon	Detailed	2
	NEA	Damascus	Syria	Detailed	2
	NIS	Minsk	Belarus	Detailed	2
	NIS	Chisinau	Moldova	Detailed	2
	NIS	Kiev	Ukraine	Detailed	2
	AF	Kinshasa	Dem. Rep. Of Congo	Detailed	2
	AF	Maseru	Lesotho	Detailed	2
	AF	Lilongwe	Malawi	Detailed	2
	AF	Maputo	Mozambique	Detailed	2
	AF	Kigali	Rwanda	Detailed	2
	AF	Pretoria	South Africa	Detailed	2
	AF	Khartoum	Sudan	Detailed	2
	AF	Mbabane	Swaziland	Detailed	2
	AF	Lusaka	Zambia	Detailed	2
	AF	Harare	Zimbabwe	Detailed	2
	EUR	Sofia	Bulgaria	Detailed	2
1/1/00 7:00 AM	AF	Luanda	Angola	Detailed	1
	AF	Cotonou	Benin	Detailed	1
	AF	Yaounde	Cameroon	Detailed	1
	AF	Bangui	Central AF Rep	Detailed	1
	AF	N'Djamena	Chad	Detailed	1
	AF	Brazzaville	Congo	Detailed	1
	AF	Libreville	Gabon	Detailed	1

Y2K Post Reporting Times

(based upon 0100 Weathervane and 12 Noon Detailed Reports)

Reporting Time (EST)	Region	Post Name	Country	Type of Report	Time Zone (+ GMT)
	AF	Windhoek	Namibia	Detailed	1
	AF	Lagos	Nigeria	Detailed	1
	EUR	Zagreb	Croatia	Detailed	1
	EUR	Prague	Czech Republic	Detailed	1
	EUR	Copenhagen	Denmark	Detailed	1
	EUR	Paris	France	Detailed	1
	EUR	Berlin	Germany	Detailed	1
	EUR	Budapest	Hungary	Detailed	1
	EUR	Rome	Italy	Detailed	1
	EUR	Vilnius	Lithuania	Detailed	1
	EUR	Luxembourg	Luxembourg	Detailed	1
	EUR	Skopje	Macedonia	Detailed	1
	EUR	Valletta	Malta	Detailed	1
	EUR	Oslo	Norway	Detailed	1
	EUR	Warsaw	Poland	Detailed	1
	EUR	Belgrade	Serbia	Detailed	1
	EUR	Bratislava	Slovakia	Detailed	1
	EUR	Ljubiana	Slovenia	Detailed	1
	EUR	Madrid	Spain	Detailed	1
	EUR	Stockholm	Sweden	Detailed	1
	EUR	Bern	Switzerland	Detailed	1
	EUR	The Hague	The Netherlands	Detailed	1
	EUR	Holy See	The Vatican	Detailed	1
	EUR	Tirana	Albania	Detailed	1
	EUR	Vienna	Austria	Detailed	1
	EUR	Brussels	Belgium	Detailed	1
	EUR	Sarajevo	Bosnia Herzegovina	Detailed	1
	AF	Niamey	Niger	Detailed	1
	NEA	Algiers	Algeria	Detailed	1
	NEA	Tunis	Tunisia	Detailed	1
1/1/00 8:00 AM	AF	Ouagadougou	Burkina Faso	Detailed	0
	AF	Abidjan	Cote d'Ivoire	Detailed	0
	AF	BanJul	Gambia	Detailed	0
	AF	Accra	Ghana	Detailed	0
	AF	Conakry	Guinea	Detailed	0
	AF	Bissau	Guinea-Bissau	Detailed	0
	AF	Monrovia	Liberia	Detailed	0
	AF	Bamako	Mali	Detailed	0
	AF	Nouakchott	Mauritania	Detailed	0
	AF	Dakar	Senegal	Detailed	0
	AF	Freetown	Sierra Leone	Detailed	0
	AF	Lome	Togo	Detailed	0
	EUR	London	England	Detailed	0
	EUR	Dublin	Ireland	Detailed	0
	EUR	Lisbon	Portugal	Detailed	0
	EUR	Reykjavik	Iceland	Detailed	0



Y2K Post Reporting Times

(based upon 0100 Weathervane and 12 Noon Detailed Reports)

Reporting Time (EST)	*Region*	*Post Name*	*Country*	*Type of Report*	*Time Zone (+ GMT)*
	NEA	Rabat	Morocco	Detailed	0
	EAP	Apia	Samoa	Weathervane	-11
1/1/00 9:00 AM	AF	Praia	Cape Verde	Detailed	-1
1/1/00 11:00 AM	WHA	Buenos Aires	Argentina	Detailed	-3
	WHA	Brasilia	Brazil	Detailed	-3
	WHA	Montevideo	Uruguay	Detailed	-3
1/1/00 11:30 AM	WHA	Paramaribo	Suriname	Detailed	-3.5
1/1/00 11:45 AM	WHA	Georgetown	Guyana	Detailed	-3.75
1/1/00 12:00 PM	EUR	Hamilton	Bermuda	Detailed	-4
	WHA	Bridgetown	Barbados	Detailed	-4
	WHA	La Paz	Bolivia	Detailed	-4
	WHA	Ottawa	Canada	Detailed	-5
	WHA	Santo Domingo	Dominican Republic	Detailed	-4
	WHA	St. Georges	Grenada	Detailed	-4
	WHA	Curacao	Netherlands Antilles	Detailed	-4
	WHA	Asuncion	Paraguay	Detailed	-4
	WHA	Port of Spain	Trinidad	Detailed	-4
	WHA	Caracas	Venezuela	Detailed	-4
1/1/00 1:00 PM	WHA	Bogota	Colombia	Detailed	-5
	WHA	Nassau	Bahamas	Detailed	-5
	WHA	Havana	Cuba	Detailed	-5
	WHA	Quito	Ecuador	Detailed	-5
	WHA	Port-au-Prince	Haiti	Detailed	-5
	WHA	Kingston	Jamaica	Detailed	-5
	WHA	Panama City	Panama	Detailed	-5
	WHA	Lima	Peru	Detailed	-5
1/1/00 2:00 PM	WHA	Belize City	Belize	Detailed	-6
	WHA	Mexico City	Mexico	Detailed	-6
	WHA	San Jose	Costa Rica	Detailed	-6
	WHA	San Salvador	El Salvador	Detailed	-6
	WHA	Guatemala City	Guatemala	Detailed	-6
	WHA	Tegucigalpa	Honduras	Detailed	-6
	WHA	Managua	Nicaragua	Detailed	-6
1/1/00 7:00 PM	EAP	Apia	Samoa	Detailed	-11