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.