United States General Accounting Office

GAO

Testimony

Before the Committee on International Relations, House of Representatives

For Release on Delivery
Expected at
10 a.m.
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/T-AIMD-00-25

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 United States. Unlike others, however, they must also assess the Y2K status of virtually every country where the United States 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 included in the appendix 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 have 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 information technology (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 that 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 traveling 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.

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

[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, e-mail, high-frequency radio, media, and Internet home page mechanisms.

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 that 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.

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,

[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.

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 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 that 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 that 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

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

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 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

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

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 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 potential Y2K problems. State officials plan for all resources to be distributed no later than December 15, 1999.

USAID BCCP Is Also Inadequate

USAID has also developed an enterprisewide 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 that 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,

[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 nonemergency 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.

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 (IG) Office has performed a comprehensive review of its agency's Y2K business continuity and contingency planning process and efforts, and a representative from the IG'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.

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 missions 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

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

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

Contact and Acknowledgements

For further information regarding this testimony, please contact Linda Koontz at (202) 512-6240 or by e-mail 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 Y2K 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 enterprisewide 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 the Year 2000, 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 Year 2000 Working Group. At USAID, we interviewed senior officials including the agency's Chief Information Officer and the Director of the Office of Information Resources Management. We performed our work in Washington, D.C., from August through 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.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Mail
Postage & Fees Paid
GAO
Permit No. GI00