United States General Accounting Office

GAO

Report to Congressional Requesters

August 1998

YEAR 2000 COMPUTING CRISIS

State Department Needs To Make Fundamental Improvements To Its Year 2000 Program

GAO/AIMD-98-162

GAO

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

Accounting and Information
Management Division

B-280443

August 28, 1998

The Honorable Harold Rogers
Chairman, Subcommittee on the Departments of
Commerce, Justice, State, the Judiciary, and
Related Agencies
Committee on Appropriations
House of Representatives

The Honorable Benjamin Gilman
Chairman
Committee on International Relations
House of Representatives

This report responds to your request that we review the Department of State's progress in solving its Year 2000 computer systems problem. On January 1, 2000, many computer systems worldwide could malfunction or produce inaccurate information simply because the century has changed. The problem is rooted in how dates are recorded and computed. For the past several decades, systems have typically used two digits to represent the year—such as "97" for 1997—to save electronic storage space and reduce operating costs. In such a format, however, 2000 is indistinguishable from 1900. The Department of State relies on a variety of information systems and networks to help it carry out its responsibilities and support business functions, such as financial management, medical assistance, visa and passport issuance, diplomatic agreements and communications, and personnel. Failure to successfully address the Year 2000 problem in time could degrade or disable State's mission-critical operations.

As agreed with your office, we assessed (1) the overall status of State's efforts to identify and correct its date-sensitive systems and (2) the appropriateness of State's strategy and actions to correct its Year 2000 problems.

Results in Brief

State has taken many positive actions to increase awareness, promote sharing of information, and encourage its bureaus to make Year 2000 remediation efforts a high priority. However, State's progress in responding to the problem has been slow. For example, of the 40 systems that State identified as mission critical and needing either converting or replacing, only 17 (about 42.5 percent) have completed renovation.

More importantly, until recently, State's Year 2000 effort lacked a mission-based perspective, that is, it had not determined its core business functions or linked these functions to its mission or to the support systems necessary to conduct these operations. Because the Year 2000 problem is primarily a business problem, agencies need to take a business perspective in all aspects of it; that is, they should identify their core business areas and processes and assess the impact of system failures. Until it takes these steps, State will not have a good basis for prioritizing its systems for the purposes of correction or developing contingency plans that focus on the continuity of operations. In responding to our draft report, State noted that it has recently determined its core business functions and linked these functions to its mission. It has not yet linked its core business functions to support systems necessary to conduct these operations.

Finally, State has not been managing the identification and correction of its interfaces effectively. Specifically, it is still identifying its interfaces, even though this task should have been completed in the assessment phase, and it has developed written agreements with data exchange partners for only a small portion of its interfaces. As a result, State has increased the risk that Year 2000 errors will be propagated from one organization's systems to another's.

Objectives, Scope, and Methodology

Our objectives were to assess (1) the overall status of State's efforts to identify and correct its date-sensitive systems and (2) the appropriateness of State's strategy and actions for remediating Year 2000 problems. In conducting our review, we assessed State's Year 2000 efforts against our Year 2000 Assessment Guide.[1] This guide addresses common issues affecting most federal agencies and presents a structured approach, as well as a checklist, to aid in planning, managing, and evaluating Year 2000 programs. This guidance describes five phases supported by program and project management activities. Each phase represents a major Year 2000 program activity or segment. The phases and a description of each follow.

- **Awareness** - Define the Year 2000 problem and gain executive-level support and sponsorship for a Year 2000 program. Establish a Year 2000 program team and develop an overall strategy. Ensure that everyone in the organization is fully aware of the issue.
- **Assessment** - Assess the Year 2000 impact on the enterprise. Identify core business areas and processes, inventory and analyze systems supporting

[1]Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997); first issued as an exposure draft in February 1997.

the core business areas, and prioritize their conversion or replacement. Develop contingency plans to handle data exchange issues, lack of data, and bad data. Identify and secure the necessary resources.

- **Renovation** - Convert, replace, or eliminate selected platforms, systems, databases, and utilities. Modify interfaces.
- **Validation** - Test, verify, and validate converted or replaced platforms, systems, databases, and utilities. Test the performance, functionality, and integration of converted or replaced platforms, systems, databases, utilities, and interfaces in an environment that faithfully represents the operational environment.
- **Implementation** - Implement converted or replaced platforms, systems, databases, utilities, and interfaces. Implement any and all contingency plans needed.

We also assessed State's efforts against our Year 2000 Business Continuity and Contingency Planning Guide, which was issued as an exposure draft in March 1998.[2] The guide provides a conceptual framework for helping large agencies manage the risk of potential Year 2000-induced disruptions to their operations. Like our Assessment Guide, it offers a structured approach for reviewing the adequacy of agency Year 2000 business continuity and contingency planning efforts.

To determine the overall status of State's Year 2000 program, we analyzed the Department of State's Year 2000 database, which includes data collected on a monthly basis from all of State's bureaus, for four separate reporting periods: August 1997, December 1997, March 1998, and May 1998. State uses this database to track and measure program progress. We also reviewed the status reports State provided to the Office of Management and Budget (OMB) on a quarterly basis. To determine how State's bureaus were implementing department policy and managing their Year 2000 program efforts, we interviewed Year 2000 coordinators at bureaus including Consular Affairs, Financial Management and Planning, Personnel, Diplomatic Security, and Information Management. We met with officials from the Diplomatic Telecommunications Service Program Office to determine what steps they were taking to ensure that telecommunications systems were Year 2000 compliant. We also reviewed internal State documents and reviews. We conducted our work from April 1997 through July 1998 in accordance with generally accepted government auditing standards.

[2]Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, March 1998, exposure draft).

We requested written comments on a draft of this report from the Secretary of State or her designee. The Acting Chief Financial Officer provided us with written comments that are discussed in the "Agency Comments and Our Evaluation" section and are reprinted in appendix I.

Background

Most of State's automated information systems are vulnerable to the Year 2000 problem, which is rooted in the way dates are recorded and computed in automated information systems. For the past several decades, systems have typically used two digits to represent the year, such as "97" representing 1997, in order to conserve on electronic data storage and reduce operating costs. With this two-digit format, however, the Year 2000 is indistinguishable from 1900, or 2001 from 1901, etc.

In addition, any electronic device that contains a microprocessor or is dependent on a timing sequence may also be vulnerable to Year 2000 problems. This includes, but is not limited to, computer hardware, telecommunications equipment, building security systems, elevators, and medical equipment.

Should State fail to address the Year 2000 problem in time, its mission-critical operations could be severely degraded or disabled as the following examples illustrate.

- The failure of State's Consular Lookout and Security System (CLASS) would hinder the ability of overseas posts to effectively screen visa applicants who may have a criminal and/or terrorist background.
- Embassy operations, such as property management and visa and passport processing, could be hindered at certain locations if State is unable to replace all of its noncompliant systems.
- State's messaging systems, which are critical to the effective conduct of diplomatic missions, could fail if telecommunications devices are not replaced or upgraded.

State has 262 systems comprising approximately 35 million lines of code written in over 17 programming languages. Major corporate systems include the Central Financial Management System (CFMS), the Central Personnel System (CPS), and CLASS. Through a strategy of system conversion and replacement, the department plans to remediate all of its noncompliant systems by March 31, 1999.

State supports its systems on a variety of hardware platforms, most of which are not Year 2000 compliant and will need to be fixed. Some of its corporate systems are operated on IBM mainframe computers at data processing centers in the Washington, D.C., area and overseas. According to State, some of its operating systems use antiquated "home grown" code and are presently not Year 2000 compliant. This environment is not stable, and State is currently working to resolve the issue.

The department also operates a variety of decentralized information technology platforms at posts around the world, including about 250 Wang VS minicomputers; 20,000 personal computers; and several hundred local area networks. Foreign service officers rely on this equipment for electronic mail, word processing, and other functions to develop reports and communicate information in support of State's foreign policy objectives.

The Wang minicomputers will be replaced as part of State's effort to modernize its information technology infrastructure. This project is known as A Logical Modernization Approach (ALMA). According to State's IRM Tactical Plan, the ALMA project will (1) ensure that legacy Wang VS equipment and software is replaced by December 31, 1999, and (2) implement modern, open, and standards-based systems throughout the department. Under the direction of State's Bureau of Information Resources Management, the department plans to deploy the ALMA infrastructure to all of State's posts by the end of fiscal year 1999.

State's Year 2000 Efforts to Date

State plans to resolve its Year 2000 problem using a phased process. In keeping with its decentralized approach to information technology management, State has charged its bureaus with responsibility for ensuring that all of their systems process dates correctly.[3] Further, State is requiring the bureaus to redirect existing funds to correct their systems and will provide no additional funds for Year 2000 remediation. Although State estimated in its May 1998 quarterly report to OMB that it would cost $153 million to address its Year 2000 problem, in commenting on a draft of this report, the department stated that it is currently collecting and analyzing cost data and that an overall figure has not been finalized.

[3]The State Department is composed of 26 bureaus that are assigned either regional or functional responsibilities. Regional bureaus are responsible for overseas posts within their respective areas. Examples include the Bureau of European and Canadian Affairs, the Bureau of African Affairs, and the Bureau of East Asian and Pacific Affairs. Functional bureaus include the Bureaus of Administration, Personnel, Financial Management and Planning, Consular Affairs, and Diplomatic Security.

State's Chief Information Officer (CIO) has overall responsibility for ensuring Year 2000 compliance. In addition, State has appointed a full-time Deputy CIO for Year 2000. The department also established a Year 2000 Steering Committee to (1) review new and ongoing information resources management (IRM) and non-IRM systems with regard to Year 2000 compliance, (2) conduct monthly reviews of Year 2000 efforts of all bureaus, and (3) reallocate resources across the department to meet Year 2000 needs as necessary. The Year 2000 Steering Committee is chaired by the Under Secretary for Management, and its membership includes the CIO, the Deputy CIO for Year 2000, the Chief Financial Officer, the Inspector General, the Assistant Secretaries of State for Diplomatic Security, Consular Affairs and Administration, and other senior officials. The CIO and the Year 2000 project manager monitor critical project implementation at key decision points and make specific recommendations to the Steering Committee. This committee meets monthly. Table 1 depicts the organizations involved in Year 2000 activities and their respective responsibilities.

Table 1: State Year 2000 Organizations and Assigned Responsibilities

Organizational component	Year 2000 responsibility
Office of the Chief Information Officer	Policy guidance and direction
Year 2000 Steering Committee	Program oversight and resource management
Deputy Chief Information Officer for Year 2000	Program management
Domestic bureaus and overseas posts	Program execution

To increase the awareness of Year 2000 problems and to foster coordination among components, State has taken the following actions.

- In an April 1996 memo, the CIO alerted bureaus to the problem and called on them to attend a meeting to discuss the issue.
- In May 1996, State established a Year 2000 Project Office to manage the department's Year 2000 program.
- In April 1997, the Year 2000 Project Office issued its Year 2000 Project Plan, which outlines the department's strategy for achieving Year 2000 compliance. Subsequently, the project office distributed formal standards and guidance, including (1) a memorandum to all application developers (both in-house and contractor) providing guidance on Year 2000 data formats governing internal and external data exchange between information systems, (2) cable notices to all overseas posts informing them about the Year 2000 problem and identifying the steps they need to

take to resolve the problem, and (3) Year 2000 planning and reporting guidance requiring bureaus to develop Year 2000 project plans and to provide quarterly (later changed to monthly) progress reports.

- In December 1997, State's Year 2000 Project Office issued draft Year 2000 test planning and certification guidance to the department. This document describes the department's Year 2000 test planning requirements, strategy, and schedule. In addition, the guidance identifies Year 2000 renovation test facilities for the IBM Mainframe, Wang, and PC/LAN test environments.
- In March 1998, State enlisted the Inspector General to help monitor its Year 2000 program, validate the data on Year 2000 status being reported by each component, identify problem areas, and recommend corrective actions.
- In March 1998, State reorganized the management of its Year 2000 effort. A Deputy CIO for Year 2000 was appointed as part of the general CIO office. The Under Secretary of State (Management) made each of the assistant secretaries personally responsible for ensuring that each of their bureaus is Year 2000 compliant.

Finally, an additional contractor, KPMG Peat Marwick LLP, was brought in to work alongside State personnel and the contractor already in place, Adsystech. KPMG Peat Marwick LLP was tasked with assisting in the overall management of the Year 2000 effort; Adsystech had been given responsibility for providing technical advice to bureaus for remediating systems. Adsystech is also responsible for collecting and analyzing data on the remediation process, and coordinating technical matters between State Department management and individual bureaus.

Using its assessment methods, State has identified a total of 262 systems, 64 mission critical and 198 nonmission critical. State has also determined that 40 mission-critical systems need to be remediated—27 of these need to be replaced and 13 need to be converted. In addition, State reports that 146[4] nonmission-critical systems need to be converted, replaced, or retired. Details of State's assessment of its systems, as reported for May 1998, are shown in table 2.

[4]Two noncompliant, nonmission-critical systems—Consular Shared Tables (CST) and Refugee Data Center (RDC)— either failed to report strategy or reported as other.

Table 2: Reported Status of State Year 2000 Efforts (as of May 1998)

	Mission-critical systems (64 systems)		Nonmission-critical systems (198 systems)	
Status as reported by State	**Number**	**Percent**	**Number**	**Percent**
Compliant	24	37.5	50	25.3
Replace	27	42.2	117	59.1
Convert	13	20.3	10	5.1
Retire	0	0	19	9.6
Other	0	0	1	.5
Not Reported	0	0	1	.5
Total	**64**	**100.00**	**198**	**100.1[a]**

[a]Percent does not total 100 percent due to rounding.

Source: State Department. We did not independently verify this information.

Inadequate Progress in Remediating Systems

State's progress in remediating systems has been inadequate. Of the 40 systems State has identified as mission-critical and is either converting or replacing, only 17 (about 42.5 percent) have completed renovation, 11 have completed validation, and only two have completed implementation. Tables 3 and 4 show the number of applications that have completed each phase along with the number of applications that have started but have not yet completed the phase.

Table 3: Reported Status of State Year 2000 Efforts for 40 Mission-Critical Noncompliant Systems (as of May 1998)

	Completed phase		In phase	
Remedial phase	**Number**	**Percent**	**Number**	**Percent**
Assessment phase	40	100.0	0	0
Renovation phase	17	42.5	18	45.0
Validation phase	11	27.5	16	40.0
Implementation phase	2	5.0	10	25.0

Note: Numbers and percents do not total to 100 percent due to State's Year 2000 reporting procedures. For example, systems with multiple components are not counted as completing a phase (the first two columns of the table) unless all components have completed the phase. However, these components may be reflected as being renovated, validated, and/or implemented (the third and fourth columns of the table).

Source: State Department. We did not independently verify this information.

Table 4: Reported Status of State Year 2000 Efforts for 146 Nonmission-Critical Noncompliant Systems (as of May 1998)

	Completed phase		In phase	
Remedial phase	**Number**	**Percent**	**Number**	**Percent**
Assessment phase	112	76.7	15	10.3
Renovation phase	50	34.2	27	18.5
Validation phase	42	28.8	16	11.0
Implementation phase	31	21.2	17	11.6

Note: Numbers and percents do not total to 100 percent due to State's Year 2000 reporting procedures. For example, systems with multiple components are not counted as completing a phase (the first two columns of the table) unless all components have completed the phase. However, these components may be reflected as being renovated, validated and/or implemented (the third and fourth columns of the table). In addition, not all nonmission-critical systems have entered the assessment phase.

Source: State Department. We did not independently verify this information.

In addition, the department has already conceded that it will not achieve its goal of eliminating all of its Wang software and hardware systems by the year 2000. As part of its IRM modernization program, State originally planned to eliminate all of its Wang VS systems (which include 21 mission-critical noncompliant systems) and begin running them on the Windows NT platform before January 1, 2000. According to State officials, however, because of delays in converting the Wang Systems to the Windows NT platform, the department will have to continue running some systems on the Wang platform after January 1, 2000. If all of the Wang systems cannot be replaced or made compliant before the year 2000, the department will not be able to run all of its mission-critical administrative applications overseas.

Further, a May 1998 report[5] found that five of the mission-critical systems reported to OMB as compliant were, in fact, noncompliant and needed some form of additional remediation.[6] The report also noted that 13 of all mission-critical systems were in a low degree of preparedness for certification and 8 systems were in a moderate degree of preparedness.[7] In addition, seven of the mission-critical systems in a low degree of preparedness were scheduled to miss the OMB milestone date for

[5]Department of State Year 2000 Management Notebook, May 27 1998.

[6]These five systems are included among the 24 mission-critical compliant systems in our tables.

[7]Degrees of preparedness were based on three factors: schedule, risk, and interfaces. Schedule reflected whether the system was on schedule for remediation. Risk reflected whether contingency plans and test plans were in place, the size of the system, and the complexity involved in remediating the system, among other risk factors. Interfaces reflected whether interfaces were appropriately identified. Thirty-nine mission-critical systems were considered to be in a high degree of preparedness for certification.

implementation by 5 months, pushing their expected implementation to September 1999. These included systems essential to citizen services, such as immigrant and nonimmigrant visa issuance and tracking, and embassy and post security. One of these systems, the Immigrant Visa System, was reported to OMB as compliant. An additional system, the Non-Immigrant Visa System, was scheduled to miss the OMB milestone date for implementation by 1 month.

State Recognizes That a Mission-Based Perspective to Year 2000 Is Needed

As noted in our Assessment Guide and our Contingency Planning Guide, the Year 2000 problem is not just an information technology problem, but primarily a business problem. Thus, the process of identifying, ranking, and remediating information systems should include an identification of core business areas and business processes and assessments of the impact of information system failures on those business areas and processes. If this is not done, the agency will not have a good basis for prioritizing systems for correction or developing contingency plans that focus on the continuity of operations.

Until recently, State's Year 2000 effort lacked a mission-based perspective. For example, at the time of our review, State had not determined its core business functions and linked these functions to its mission or to its support systems. In addition, the department had not conducted formal risk analyses of the majority of its systems. In responding to a draft of this report, State noted that it is currently developing a framework for a mission-based perspective for its Year 2000 problem. It has recently determined its core business functions and linked these functions to its mission. However, it has not yet linked its core business functions to support systems necessary to conduct these operations.

As further illustrated below, until it fully adopts this perspective, State will not be able to adequately prioritize its systems or develop meaningful contingency plans.

State Has Not Effectively Prioritized Systems for Correction

According to our Assessment Guide, an important aspect of the assessment phase is determining and prioritizing the correction of the systems that have the highest impact on an agency's mission and thus need to be corrected first. This helps an agency ensure that its most vital systems are corrected before systems that do not support the agency's core business.

State has provided its bureaus with a definition of priorities—routine, critical, and mission-critical—and charged them with the task of identifying and ranking their respective systems according to this definition. Mission critical, the highest priority, was defined as crucial to worldwide operations, affecting the public directly, or having national security implications. Subsequently, the bureaus assessed their respective systems and each provided the Year 2000 Project Office with a list of systems—64 in total[8]—that they determined were mission-critical to department operations.

However, this process is flawed because it provides no means of distinguishing between individual bureaus' priorities—some of which are essential to State's core mission and some of which are not. For example, the following systems have been ranked by individual bureaus as mission critical:

- REGIS, a system designed to register and track students who attend the Foreign Service Institute;
- MSE Network, a system used to sort and track unclassified mail and parcels;
- CLASS, a system designed to identify criminals and possible terrorists in order to block their entry into the United States;
- CRIS, an on-line database used to track citizens involved in crises overseas; and
- ICARS, a system used for immigration control and reporting.

Clearly, CLASS, CRIS, and ICARS are much more important to State's core missions than REGIS and MSE. But under State's Year 2000 approach, they rank equally. Until State begins focusing on core business areas and processes, it will not have a basis for further ranking these systems for remediation.

Additionally, it appears that State has not placed enough priority on fixing its mission-critical systems before its nonmission-critical systems. In fact, as tables 3 and 4 indicate, State is making better progress on its nonmission-critical systems than on its mission-critical systems. For example, 31, or 21 percent, of nonmission-critical systems have reportedly completed the implementation phase, while only 2, or 5 percent, of mission-critical systems have done so.

[8]State assessed 24 of these systems as Year 2000 compliant and 40 as needing either replacement or conversion.

State officials agree that the current prioritization process is flawed. In responding to a draft of this report, the department stated that it had recently identified its core business functions and planned to link them to the 64 systems previously identified as mission critical, thereby providing a functional basis for prioritizing their efforts. However, State did not plan to reassess the 198 systems previously identified as nonmission-critical using its new mission-based approach. Without reassessing all of its systems, State will not be able to fully ensure that the most critical functions will not be disrupted by the Year 2000 problem.

Business Continuity and Contingency Planning Is Inadequate

To mitigate the risk that Year 2000-related problems will disrupt operations, our guide on business continuity and contingency planning recommends that agencies perform risk assessments and develop realistic contingency plans during the assessment phase to ensure the continuity of critical operations and business processes. Contingency plans are vital because they identify the manual or other fallback procedures to be employed should systems miss their Year 2000 deadline or fail unexpectedly. These plans also define the specific conditions that will cause their activation.

State has directed its bureaus to develop written contingency plans for all mission-critical systems. At the time of our review, State reported that 16 written plans had been prepared, covering less than half of the 40 systems State identified as mission-critical and noncompliant. However, State was able to provide us with only six of these plans. These plans included only brief risk assessments and summary statements about possible alternate approaches for providing system functionality. They did not discuss the impact of the failure of system functionality on State's mission.

Furthermore, State's contingency planning is insufficient because it has not focused on ensuring the continuity of department operations and business processes. As noted in our Contingency Planning Guide, the risk of failure is not limited to an organization's internal information systems. Many federal agencies also depend on information and data provided by their business partners—including other federal agencies, state and local agencies, international organizations, and private sector entities. In addition, they depend on services provided by the public infrastructure—including power, water, transportation, and voice and data telecommunications. Because of these risks, agencies must not limit their contingency planning effort to the risks posed by the Year 2000-induced failures on internal information systems. Rather, they must include the

potential Year 2000 failures of others, including business partners and infrastructure service providers. By focusing only on its internal systems, State will not be able to protect itself against major disruptions of business operations.

In its May 1998 quarterly report to OMB on the status of its Year 2000 program, State acknowledged that its contingency planning efforts to date have focused on information technology systems rather than on the "larger picture of continuity of business operations." To strengthen contingency planning, State has established a business continuity work group which includes members from the Year 2000 Steering Committee and is chaired by the Under Secretary for Management. This group is responsible for the development of business continuation strategies for Year 2000 risks. State has not identified a deadline for this group to complete its work.

State's Management of Interfaces Has Been Ineffective

State systems interface with each other as well as with systems belonging to other federal agencies and international entities as shown in the following examples.

- State's central messaging system, which is used to transmit official diplomatic cables to overseas posts and other U.S. sites worldwide, interfaces with the Department of Defense.
- State's central personnel system interfaces with its payroll system to support payroll processing functions.
- State's CLASS system receives data on persons wanted for, or convicted of, drug-related crimes from the Drug Enforcement Agency's (DEA) Lookout System.

As a result, it is essential that State ensure that all of its interfaces are Year 2000 compliant and that noncompliant interfacing partners will not introduce Year 2000-related errors into compliant State systems. Our Year 2000 Assessment Guide recommends that agreements with interface partners be initiated during the assessment phase to determine how and when interface conflicts will be resolved.

State has not managed the identification and correction of its interfaces effectively. First, it is still in the process of identifying its interfaces, even though our Year 2000 Assessment Guide recommended that this be done during the assessment phase. At the time of our review, State had identified 12 interfaces between mission-critical and external systems belonging to State and other agencies and organizations and 28 internal

interfaces between bureaus that are affected by the Year 2000 problem. In addition, in June 1998, State reported to the President's Council on Year 2000 Conversion that it maintained interfaces with commercial banks in 157 countries. According to State, 17 percent of its overseas accounts were Year 2000 compliant, 48 percent were scheduled to be compliant by December 1998, 7 percent in March 1999, 3 percent in June 1999, and 22 percent in December 1999. Three percent of the accounts were reported as having inadequate compliance plans.[9]

However, State recently acknowledged that it could not identify every interface with other agencies or among the bureaus or verify whether all system owners were reporting on their interfaces or reporting correctly. State is now in the process of identifying these interfaces and verifying their progress.

Second, State has made little progress in developing agreements with its interface partners, which our Year 2000 Assessment Guide also recommended be done in the assessment phase in order to allow enough time for conflicts to be resolved. As of May 1998, State's bureaus were reporting that Memorandums of Understanding had been completed for only 10 interfaces for systems that it has assessed as mission critical and noncompliant.[10] Until it has agreements in place for the remaining interfaces, State will not have assurance that partners are working to correct interfaces effectively or in a timely manner.

Moreover, a May 27, 1998,[11] report listed seven mission-critical systems as having a low degree of preparedness for Year 2000 certification based on the condition of their interfaces.[12] The report also found problems with 20 other mission-critical systems due to interface problems.

Conclusions

The effective conduct of State operations hinges on its ability to successfully remediate its mission-critical computer systems before the Year 2000 deadline. While State has taken a number of actions to address this issue, its progress in several critical areas has been inadequate: only

[9]For these accounts, State has contingency plans in place to continue banking in the event of Year 2000 failures.

[10]These do not include the overseas commercial bank interfaces for which State plans to obtain corporate certification of Year 2000 compliance.

[11]Department of State Year 2000 Management Notebook, May 27, 1998.

[12]Three systems were rated as low in preparedness for both interface and scheduling problems: Telecommunications Manager, Distributed Name Check, and Immigrant Visa System.

17 of 40 systems that State has designated as mission-critical have completed renovation and it has not yet identified all of its interfaces. Further, if State continues its current approach, which lacks a mission-based perspective, it will risk spending time and resources fixing systems that have little bearing on its overall mission. It will also not be prepared to respond to unforeseen problems and delays.

Recommendations

We recommend that the Secretary of State ensure that senior program managers and the Chief Information Officer:

(1) Reassess all of State's systems using the new mission-based approach to identify those systems supporting the most critical business operations.

(2) Ensure that systems identified as supporting critical business functions pursuant to recommendation 1 receive priority attention and resources over those systems that do not support critical business functions.

(3) Redirect its contingency planning efforts to focus on the core business functions and supporting systems, particularly those supporting systems that are already scheduled to miss the OMB milestone date for implementation.

(4) Ensure that the bureaus have identified and corrected interfaces and developed written memorandums of agreement with interface partners.

Agency Comments and Our Evaluation

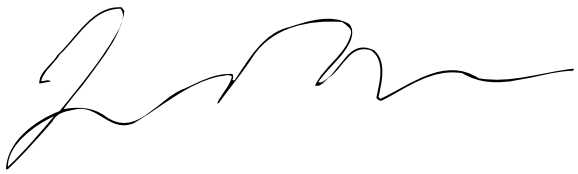
State generally agreed with the conclusions and recommendations in our report. The department noted that it has already begun to respond to our observations and recommendations and that many of the specific concerns we raised have been independently identified by the department's own consulting firm, KPMG Peat Marwick LLP. Additionally, State provided updated information about its management initiatives to address the Year 2000 problem, stating that it is rapidly implementing corrective measures for the problems cited in our report. While these changes demonstrate increased management awareness and attention to the Year 2000 problem, it will be critical for the department to follow through on these initiatives and ensure that they have a positive impact on the remediation, testing, and implementation of systems.

Furthermore, the department noted in its comments that it has recently identified its core business functions and linked these functions to its

mission. The department also stated that it planned to link its core business functions to the 64 systems previously identified as mission critical. However, State did not plan to reevaluate the 198 systems previously identified as nonmission-critical. Until State applies its new mission-based perspective to all of its systems, it will not be able to fully ensure that the most critical functions will not be disrupted by the Year 2000 problem.

We are providing copies of this letter to the Ranking Minority Members of the Subcommittee on the Departments of Commerce, Justice, State, the Judiciary and Related Agencies, House Committee on Appropriations, and the House Committee on International Relations. We are also sending copies to the Chairmen and Ranking Minority Members of the Senate Special Committee on the Year 2000 Technology Problem, the Subcommittee on Commerce, Justice, and State, the Judiciary, and Related Agencies, Senate Committee on Appropriations, Senate Committee on Governmental Affairs, the Subcommittee on Government Management, Information and Technology, House Committee on Government Reform and Oversight, and the Subcommittee on Civil Service, House Committee on Government Reform and Oversight. We are also sending copies to the Secretary of State, the Director of the Office of Management and Budget, and other interested parties. Copies will be made available to others upon request.

If you have any questions on matters discussed in this report, please call me at (202) 512-6240. Major contributors to this report are listed in appendix II.



Jack L. Brock, Jr.
Director, Governmentwide and Defense Information Systems

Comments From the Department of State

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

United States Department of State

Chief Financial Officer

Washington, D.C. 20520-7427

July 30, 1998

Dear Mr. Dodaro:

We appreciate the opportunity to review your draft report, "Year 2000 Computing Crisis: State Department Needs to Make Fundamental Improvements to Its Year 2000 Program," GAO/AIMD-98-162, GAO Job Code 511619.

Enclosed are the Department's comments. If you have any questions concerning this response, please call Mr. David Ames, IRM/Y2K Program Management Office, at (202) 647-2000.

Sincerely,

Kathleen J. Charles, Acting

Enclosure:
As stated.

cc:
GAO - Ms. Canjar
STATE/IRM/Y2K- Mr. Ames

Mr. Gene L. Dodaro,
Assistant Comptroller General,
Accounting and Information Management Division,
U.S. General Accounting Office.

Department of State's Comments of the GAO Draft Report "Year 2000 Computing Crisis: State Department Needs to Make Fundamental Improvements to Its Year 2000 Program," GAO Job Code 511619

GENERAL COMMENTS

The GAO Report to Congressional Requesters on the Department of State's (DoS) Year 2000 Crisis represents months of dedicated effort and substantial investment on the part of GAO. Since the report is scheduled for release in August, 1998, there will be considerable time elapsed between the conclusion of the audit and the report's release. In an effort to provide GAO, Congress and the Public the most accurate and relevant information on this critical issue, the following information is presented to clarify and update GAO's findings.

The GAO report is informative and thorough, and provides a fair assessment of DoS efforts prior to the appointment of a new Chief Information Officer (CIO) and the reorganization of the Year 2000 Program Management Office (PMO) under a newly established Deputy CIO for Year 2000. The following issues relate directly to the major concerns expressed in the GAO report:

- Documenting quantum changes occurring in DoS's Year 2000 Program Management Office;
- Updating the accuracy of GAO's data regarding systems' compliance status, and;
- Illustrating DoS Year 2000 initiatives which specifically address GAO's major concerns in the areas of interfaces identification and management, contingency planning, and mission-based system prioritization.

The GAO report showed that the Year 2000 problem is far-reaching and deeply embedded. However, DoS is rapidly implementing corrective measures. The Department has embraced sound management practices and incorporated repeatable, proven remediation methodologies. The resultant progress since GAO completed its study in May 1998 is substantial. Information regarding Year 2000 remediation is typically perishable because of the magnitude of change occurring within a short time frame. Therefore, it is critical the GAO is provided the most current information to accurately reflect the Department's progress and provide the Congress with the most relevant data.

The GAO report was comprehensive and focused on providing Congress and DoS invaluable insight and guidance regarding its Year 2000 program and status. It was based on the best information available at the time of audit. The methodologies provided an excellent framework within which to view the Year 2000 challenge and the perspective of a third party observer was valuable in accurately assessing the state of DoS's Year 2000 program. DoS is in general agreement with the conclusions and recommendations of the GAO report dated August 1998.

There were several discrete themes contained in the GAO report. These themes addressed broad issues important to the success of the Year 2000 effort. Specifically, GAO posited:

- DoS has not determined its mission critical, core business functions
- DoS lacks a mission-based perspective in prioritizing system remediation
- Business continuity and contingency planning is inadequate
- The identification and correction of DoS interfaces has not been effectively managed

RECENT DEPARTMENT IMPROVEMENT INITIATIVES

The observations and recommendations of the GAO audit team did not go unheeded. Over the past three months, DoS has made significant strides in meeting the Year 2000 challenge. In April of this year, the Department of State brought KPMG Peat Marwick LLP on board to provide world class program management consultative and business advisory services to the Department. One of the first tasks accomplished by KPMG was to independently identify opportunities to improve the management of the Year 2000 challenge at both the Department and Bureau. In many instances, specific concerns raised by the GAO were independently identified by KPMG.

Subsequent to the KPMG report, many of the concerns had been fully addressed, or corrective measures initiated. Specific management programs have been instituted and renewed emphasis from the highest levels of the Department on overcoming the Year 2000 problem has permeated the Department's information systems infrastructure. There has been a fundamental change in the way DoS views its core business functions, prioritizes its efforts and manages its interface identification and correction efforts. Formal Year 2000 management structures have also been established reflecting the criticality of this issue to DoS management. Specifically, Department has taken the following concrete measures since the conclusion of the GAO audit which have resulted in tangible program improvements:

1. Increased Department emphasis on the Year 2000 challenge
   - Increased Under Secretary for Management involvement
   - Creation of the Year 2000 Program Management Office reporting directly to the CIO
   - Year 2000 challenge elevated to dedicated Deputy CIO level
   - Assistant Secretaries now accountable for Year 2000 efforts
   - Monthly Year 2000 Steering Committee meetings chaired by the Under Secretary for Management and attended by Assistant Secretaries monitor status and certification

2. Enhanced Management Capability
   - New Year 2000 management infrastructure established to collect, analyze, track and report status of mission critical system remediation
   - Year 2000 assessment criteria are now standards-based
   - Progress toward Year 2000 and beyond managed through the War Room concept

3. Aggressive Focus on Certification
   - Mission critical application prioritization effort underway based on Departmental Strategic Plan
   - Year 2000 certification criteria developed jointly with the DoS Office of the Inspector General
   - Certification pilot programs are currently underway for several mission critical systems

A concerted, coordinated and structured management effort has transitioned the DoS Year 2000 program to a substantially different entity. The efforts at DoS have undergone a fundamental shift in approach and level of intensity. Formal Year 2000 corrective processes have been instituted to systematically deal with the issues effectively on a department-wide basis. Each application is now evaluated against assessment criteria including schedule, risks, interfaces test plans and contingency plans. Detailed assessments and supporting data are now provided to application owners in a Year 2000 Program Management Notebook. A better understanding of issues surrounding the Year 2000 problem has facilitated faster progress towards certification preparedness. Finally, a fully defined certification process has been reviewed and institutionalized by the DoS Inspector General, along with the Year 2000 Program Management Office.

SPECIFIC COMMENTS

Now on p. 15.

The DoS believes it has made significant progress and improvements in addressing the Year 2000 challenge. Specific DoS clarifications or comments are presented in response to the numbered recommendations on pages 24-25 of the Draft GAO report, as well as GAO comments *(which appear in italics)*. Supporting documents are available upon request.

Now on p. 15.

RECOMMENDATION (1) - Page 24:

Now on p. 2.

GAO Statement - Page 2
State has not yet determined its core business functions essential to mission and "lacks" mission-critical perspective. The result is ineffective prioritization of systems to be corrected. .

Concur.

The Department of State is currently in the process of prioritizing the 60 Mission Critical applications. The DoS prioritization framework is based on a top down approach leveraging both the Department of State Strategic Plan and the IRM Strategic Plan. The DoS intends to a have a high-level prioritized list of Mission Critical applications by 1 September 1998.

Now on p. 10.

GAO Statement - Page 16:
"State, however, has not yet determined its core business functions, linked these functions either to its mission or to support systems necessary to conduct these operations."

Partially concur.
The Department of State has used the DoS Strategic Plan and IRM Strategic Plan as the basis for identifying its core business functions. This top down approach to identifying these functions has helped the Department develop a mission based prioritization framework to facilitate identification of core business processes and underlying application support.

Now on p. 15.

RECOMMENDATION (2) - Page 25:

Now on p. 12.
See comment 1.

GAO Statement - Page 12:
"Using its assessment methods, State has identified a total of 262 systems, 64 mission critical and 198 non-mission critical. State has also determined that 40 mission-critical systems need to be remediated-27 of these need to be replaced and 13 need to be converted."

Non-concur.
The following updated information is provided after identification and application of updated mission based criteria. Total systems = 262. Mission critical systems = 60. Non-mission critical systems = 202. The DoS does not have any certified Year 2000 compliant applications. All applications within the DoS will be certified using a Department Certification and Test process.

Now on p. 11.

GAO Statement - Page 17:
"State has provided its bureaus a definition of priorities...However, this process is flawed because it provides no means of distinguishing between its individual bureaus' priorities-some of which are essential to State's core mission and some of which are not."

Partially concur.
The Department of State has developed a draft prioritization frame work which is linked to the mission of the Department as defined in the DoS Strategic Plan and the IRM Strategic Plan. The Department is currently in the process of implementing this frame work by meeting with each bureau individually to gain feedback on the process and begin aligning their application with a priority according to the criteria set forth in the

framework. This process will culminate with gaining concurrence from the Assistant Secretaries on the priority of the Department's applications in order to direct attention and resources to the highest priority applications.

Now on p. 11.

GAO Statement - Page 18:
"Additionally, it appears that State has not placed enough priority on fixing its mission-critical systems before its non-mission critical systems."

See comment 2.

Partially concur.
There may be some confusion on the manner in which status and strategy information has been reported in the past. We believe the confusion and inconsistency in reporting is in large part due to a misunderstanding of the term compliant. To date, the Department has no Y2K certified mission critical or non-mission critical applications. The Department has, however, reported a number of applications that are employing "compliant" as a strategy for remediating their applications. This means the bureau has determined the application has no date sensitive processes, is able to work with four-digit dates, or has been vendor certified compliant.

The Department of State has identified its mission critical systems and is aggressively working and managing the remediation efforts of each. Currently, the DoS Y2K War Room focuses only on the MC applications and their progress toward remediation. These applications have received the full attention of the Under Secretary for Management, the CIO, and the Y2K PMO, and they will continue to have their efforts monitored closely

Now on p. 15.

RECOMMENDATION (3) - Page 25:

Now on p. 2.

GAO Statement - Page 2:
State's business continuity and contingency planning for Y2K disruptions of mission critical operations is inadequate.

See comment 3.

Partially Concur.
The Department's approach to developing continuity of operations plans currently is a bottom-up approach by developing continuity of operations plans at the application level.

The CIO has asked for and received several contingency plans from bureaus specifically for individual MC applications. These plans are intended to serve as an IT alternative in the event an application has not been adequately remediated. Although we have not received written contingency plans for each MC application, we do expect to receive these from the bureaus in the near future. Additionally, a continuity of operations plan is being developed for each application and will be submitted in writing to the PMO. These plans must be completed prior to an application being certified by the Department.

Now on p. 15.

RECOMMENDATION (4) - Page 25:

Now on p. 2.

GAO Statement - Page 3
"Finally, State has not been managing the identification and correction of its interfaces effectively. Specifically, it is still in the process of identifying its interfaces, even though this task should have been completed in the assessment phase, and it has developed written agreements with data exchange partners for only a small portion of its systems"

Concur.
The DoS has established a management framework to identify and monitor the status of internal and external interfaces. The DoS has significantly increased visibility of, and attention to the Year 2000 system interface issue. Major corrective measures include increased production of Memoranda of Understanding (MOU) with internal and external interface partners, and technical mapping of mission critical interface points department-wide. The Department has mapped comprehensive diagrams depicting interface junctures. This approach to system interface mapping has effectively established a structured and repeatable management process for analysis and tracking the remediation progress of individual application interfaces. Additionally, the PMO has initiated efforts to define a more rigorous interface assessment process and scrutinize interface identification criteria more closely. These efforts represent significant progress in the DoS effort to improve Year 2000 interface management. As evidence of our progress, we have included both an inventory of the interfaces we are currently managing and copies of draft and finalized MOUs for selected internal and external interfaces.

Now on p. 13.

GAO Statement - Page 22:
"State has not managed the identification and correction of its interfaces effectively [overseas commercial banks]."

See comment 4.

Partially concur.
The DoS is actively managing its commercial bank interfaces throughout the world. The Under Secretary of State for Management has remained personally involved with this issue and apprised of its status. A comprehensive baseline assessment was completed and presented at the June Monthly Year 2000 Steering Committee meeting attended by the Undersecretary for Management and Bureau Assistant Secretaries. This briefing provided an inventory, status and analysis of the level of current and planned compliance with Year 2000 efforts.

ADDITIONAL COMMENTS

Now on p. 5.

GAO Statement - Page 7:
"State plans to complete the installation and testing of Year 2000 compliant operation system software for all of its IBM mainframe computers by the end of July, 1998."

6

Non-concur.
Based on our latest information, all IBM mainframe operating systems will be compliant by August 31, 1998. Currently, there are eighteen Logical Partitions. Eleven of them are using IBM's Y2K ready operating system and seven of them are not. These systems utilize antiquated, "home grown" code and at the present time, the environment is not stable. Major resources from Department personnel, contractors and vendors have been applied towards resolving this issue.

Now on p. 5.

GAO Statement - Page 9:
"As of May 1998, State estimated that it would cost $153 million to address its Year 2000 problem."

See comment 5.

Non-concur.
The DoS is currently collecting and analyzing data for FY 2000 Y2K estimates; an overall figure for DoS has not been finalized.

Now on p. 7.

GAO Statement - Page 11:
"State reorganized the management of its Year 2000 effort."

Concur.
In March 1998, the Under Secretary for Management increased the emphasis of Year 2000 corrective actions within the Department by making Assistant Secretaries who own Mission Critical applications fully accountable for compliance of the systems within their individual Bureaus. Monthly Year 2000 Steering Committee Meetings are conducted and chaired by the Under Secretary to review the status of all Mission Critical applications as well as other key Year 2000-related initiatives. Additionally, a new department CIO was appointed in May 1998, and the new post of Deputy CIO for Year 2000 was created. The Year 2000 Program Management Office underwent significant overhaul resulting in more focused and effective program management. KPMG was also brought on board to assist in the management of Year 2000 efforts.

The following are GAO's comments on the Department of State's letter dated July 30, 1998.

GAO Comments

1. State's detailed statistical information about its Year 2000 effort is constantly changing as State's Year 2000 program evolves and remediation efforts progress. The information in our report represents the official figures reported to OMB in May 1998. The figures that State claims are more current are not substantially different from those reported in May 1998 and would not have any significant impact on our findings and recommendations.

2. Our assessment of the relative priority of fixing mission-critical and nonmission-critical systems did not include systems that State had designated as "compliant." Instead, this assessment is based on the comparative number of noncompliant mission-critical and nonmission-critical systems that have completed the implementation phase. Only 2 (5 percent) of the 40 mission-critical noncompliant systems had been implemented as of May 1998 whereas 31 (21 percent) of the 146 nonmission-critical noncompliant systems had been implemented. We agree that systems currently considered "compliant" may not actually meet criteria for compliance and need to undergo their own, separate certification process.

3. State's comments indicate that it is still taking a flawed approach to contingency planning. Like the prioritization of systems, contingency planning needs to be a top down rather than a bottom up process. That is, agencies must first identify their core business processes and assess the Year 2000 risk and impact of these processes. Subsequently, they can develop plans for each core business process and infrastructure component. As noted in our Year 2000 Contingency Planning Guide, this approach enables agencies to consider and mitigate risks that extend beyond individual applications or systems. For example, as noted in our report, State depends on information and data provided by other federal agencies, international organizations, and private sector entities. It also depends on services provided by the public infrastructure, including power, water, transportation, and voice and data telecommunications. Neither of these dependencies will be considered if contingency planning is focused on individual internal systems.

4. State provided no evidence of increased identification and awareness of commercial bank interfaces. Neither could the Department identify the number of international interfaces it might have.

5. In May 1998, State reported to OMB that its estimated cost to address its Year 2000 problem was $153 million. In our final report, we have noted that State no longer considers this figure to be accurate.

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.

John Deferrari, Assistant Director
Frank Deffer, Assistant Director
Brian Spencer, Technical Adviser
R.E. Canjar, Evaluator-In-Charge
Cristina Chaplain, Communications Analyst

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

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested