



---

**UNITED STATES INTERNATIONAL TRADE COMMISSION**

---

WASHINGTON, D.C. 20436

July 23, 1999

## MEMORANDUM

TO: Chairman

FROM: Acting Inspector General 

SUBJECT: Inspection Report 05-99, Follow-up Review of Commission's Preparation for the Year 2000

The Office of Inspector General (OIG) conducted a follow-up inspection to Audit Report 03-99 *Evaluation of the Commission's Preparation for the Year 2000* (Y2K) to assess the International Trade Commission's (Commission) progress in Year Y2K activities.

The objectives of this inspection were to review the progress made by the Commission in implementing recommendations and suggestions made in Report Number IG-03-99 and to identify areas wherein the Commission could be more proactive to minimize disruption because of the Y2K issues.

OIG generally found that the Commission has made significant progress since the time of our audit. The Director of Operations, as the Commission's Y2K official, was given the opportunity to comment on a draft of this report and his comments were appropriately incorporated. Specific findings are contained in the report and our suggestions for continued progress are found on page 6.

Attachment

cc: Commission  
Office Directors (Email distribution)

**OFFICE OF INSPECTOR GENERAL**

**Follow-up Review of Commission's Preparation for the Year 2000**

**Inspection Report IG-05-99**



Date: July 23, 1999

## I. INTRODUCTION

The United States International Trade Commission (Commission) provides advice to the President and Congress on tariff and trade matters, conducts investigations relating to the impact of imports on domestic industries, and contributes to the development of U.S. trade policy. The Commission has approximately 388 employees and a fiscal year (FY) 1999 budget of approximately \$45 million.

Since 1988, the Commission has automated essential agency functions and implemented an enterprise-wide local area network. Consequently, the Commission relies upon several information systems and its underlying enterprise network to perform its mission. The Commission depends on information systems developed by other Federal agencies to perform its financial responsibilities, pay its employees, and perform its personnel management functions. The Commission uses information-gathering systems from commercial organizations for news and legal research. The Commission uses components that contain embedded electronics. The electronics are found in the building infrastructure, telephone and fax systems, and in the audio-visual systems used in the Commission's hearing rooms.

At 12:01 a.m. on January 1, 2000, many computer systems, electronic devices and components that contain embedded electronics could malfunction or produce incorrect information simply because the date has changed. The year 2000 (Y2K) problem is rooted in the way dates are recorded and computed in many computer systems and other electronic components. For the past few decades, systems have typically used two digits to represent the year, such as "97" representing 1997. With this two-digit format, the year 2000 is indistinguishable from 1900, the year 2001 from 1901, and so on. As a result of this ambiguity, electronic components and computer hardware, operating system software, application software, application programs, and data that use dates to perform calculations, comparisons, or sorting may fail or generate incorrect results.

On January 1, 2000, the ability of the Commission to accomplish its mission without disruption is at risk unless the information systems and components on which the Commission depends are Y2K compliant. Minimizing the impact of the Y2K problem on the Commission requires an organized managerial and technological effort. Otherwise, the Commission may have to perform its work using manual methods, processes, and procedures.

## II. BACKGROUND

The Office of Inspector General (OIG) initially audited the Commission's Y2K activities in the winter of 1998 and submitted *Evaluation of the Commission's Preparation for the Year 2000*, Report Number IG-03-99 in February 1999. That report found that the extent of the Y2K problem on Commission operations was not documented or well understood and concluded that the Commission will likely experience some disruption because of the Y2K problem. The report recommended that the Chairman appoint a single Y2K official to manage the Commission's Y2K activities. The report further recommended that the Y2K official:

- Ensure that all systems susceptible to Y2K problems have been identified;
- Assemble an integrated project team consisting of a representative for each mission-critical system;
- Develop a Y2K policy establishing the Commission's acceptable level of risk;
- Increase awareness of the Y2K problem among Commission employees, and
- Develop and implement a Y2K action plan.

This Inspection conducted in late June 1999 is a follow-up review to assess the Commission's progress with regard to the earlier audit recommendations.

## III. OBJECTIVES

The objectives of this Inspection were to:

- review the progress made by the Commission in implementing recommendations and suggestions made in Report Number IG-03-99, *Evaluation of the Commission's Preparation for the Year 2000*;
- identify areas wherein the Commission must be more proactive to minimize disruption because of the Y2K problems.

## IV. METHODOLOGY

Burke Consortium, Inc. (BCI) developed data-gathering templates for each recommendation and provided a copy of these templates to Commission officials responsible for each system. During the week of June 21, 1999, BCI met with each responsible official to:

- review the status of current remediation efforts;
- identify the scope of work performed since the previous review;
- identify the actions that remain to be completed; and
- identify the timeliness of the schedules for completion.

In addition, BCI conducted random spot checks of components used in the Commission to assess the degree of Y2K compliance.

**V. FINDINGS**

The Commission has made significant progress since the review conducted during the winter of 1998. The Chairman designated the Director, Office of Operations as the Commission's Y2K official. The Y2K official established a Y2K Committee to monitor overall Y2K progress and provide bi-weekly reports of progress to the Chairman. The Y2K Committee completed a survey of each office that identifies the most important functions that need to be protected from disruption due to Y2K problems. This survey identifies critical work products that each office will have to produce during January 2000, and the Y2K-vulnerable systems that are used to prepare the products. Information gathered during this survey served as the basis from which the Y2K Committee identified the Commission's critical business processes and associated information systems. The Y2K Committee used the results of this survey to identify the Commission's mission critical "first tier" and "second tier" functions.

**FINDINGS**

- The Commission has made significant progress.
- The Commission has identified mission-critical processes and associated information systems.
- The Commission has updated the inventory of all information systems and has completed remediation of many mission-critical components.
- The Commission has completed an Action Plan with a Master schedule of Y2K events.
- The Commission has begun high-level contingency planning for all mission-critical processes.

The Commission identified "first tier functions" as those that must operate during any potential disruption or the agency may face serious adverse consequences. The Commission's first tier functions are: (1) building security, (2) payroll, (3) remediation of Y2K problems, and (4) basic communications. The Commission identified "second tier functions" as those that are crucial to the Commission's long-term operations, but during January 2000, potentially could be postponed in the event of a massive disruption. The Commission's second tier functions also include investigation and research activities that fulfill the agency's mission.

The Office of Information Services (OIS) completed an inventory of Commission software and hardware for Y2K review. The inventory listing reflects the remediation status of all systems and components. However, a spot check revealed that some items which should be identified and tracked for Y2K compliance were not included in the current inventory listing. The items have been added to the inventory. Procedures are now in place to ensure that system changes are Y2K compliant and added to the inventory upon installation.

OIS has completed remediation on all 400-plus personal computers (PCS) and many mission-critical components. A random spot check of components noted as compliant on the inventory list revealed that all were compliant per manufacturer recommendations. The Office of Publishing (PUB) has completed remediation on the entire publishing system.

The Commission provided a high-level Y2K Contingency Plan to OMB on June 15, 1999. Detailed contingency planning for all first and second tier functions is scheduled to begin in July and be completed by September. Detailed contingency plans will take into account three scenarios that correspond to major levels of possible disruption: (1) The agency has no power and/or water, thus precluding use of the building; (2) the agency has power, water, and PCS, but no network, communications (telephones, facsimile, e-mail), or duplication capability (copiers, Docutech); and (3) the agency has power, PCS, copies, and the network (including internal e-mail), but no external communications (telephones, Internet, facsimile, external e-mail).

For tier one functions, the Y2K Committee has tasked Director of Administration, Director of OIS and Director of External Relations to develop a contingency plan based on the scenarios listed above. Additionally, for tier two functions, the five Business Continuity and Contingency Planning team leaders (the Director of Investigations, the Director of Unfair Import Investigations, the Director of Industries, the Director of Tariff Affairs and Trade Agreements, and the Director of External Relations) have been tasked to develop a contingency plan for each business operation.

The Action Plan finalized on July 2, 1999 identifies remaining work, assigns target dates for completion, assigns responsibility for completing remaining actions, and serves as the Commission's master schedule of Y2K related actions. See Appendix A.

Follow-up reviews of the Commission's mission-critical systems were conducted in order to determine progress since the review conducted during the winter of 1998. Significant progress has been made on all mission-critical systems. A summary of eight systems is provided below.

#### 1. Accounting/Payroll/Personnel

The Chief, Finance Division, Office of Finance and Budget (OFB) was contacted to obtain the status of this system. Roles and responsibilities between the OFB, the Office of Personnel, and the OIS for ensuring Y2K compliance of "non-standard" workstation hardware, software, and other components have been defined. OFB will serve as liaison with other government agencies for all components that are their responsibility as providers of accounting and payroll systems services to the Commission. OIS will service and maintain "non-standard" components, such as older 80486-based machines, that are the Commission's responsibility. OFB personnel are working with the providers of accounting,

---

*“OFB personnel are awaiting instructions from the Director of Administration to begin developing formal internal procedures for processing employee payroll.”*

---

payroll, and personnel system services, the Department of Treasury and the Department of Interior, to prepare contingency plans for essential functions in the event that accounting, payroll, or personnel systems fail. These plans will include procedures for faxing and mailing information in the event that these systems are not available. OFB personnel are awaiting instructions from the Director of Administration to begin developing formal internal procedures for processing employee payroll. OFB personnel are awaiting receipt of new Y2K compliant software for the

Government On-Line Accounting Link System, used to receive government bills, meet reporting requirements, and perform other financial-related functions. OFB personnel anticipate receiving and installing the new software by the end of July.

#### 2. ITC Net

The Chief, Information Systems Division and OIS Computer Specialist were contacted to obtain the status of this system. Roles and responsibilities for Y2K compliance have been assigned. An inventory of ITC Net hardware and software components has been prepared. Critical components have been identified. Renovation has been performed on most critical components, with the remainder scheduled to be completed by July 30, 1999. Renovation of all components is scheduled to be complete by September 30, 1999. There will not be a continuity plan developed specifically for ITC Net. ITC Net services will be incorporated into continuity plans being prepared by the Tier 2 business process owners.

### 3. PCS and COTS

The Chief, Information Systems Division and OIS Computer Specialist were contacted to obtain the status of this system. Significant progress has been made since the initial review. Roles and responsibilities for Y2K compliance have been assigned. The OIS has validated the inventory of PCS and commercial-off-the-shelf software (COTS), and has renovated all Dell PC hardware and ITC standard software, with the exception of Microsoft Access 95, which will be upgraded to a Y2K compliant version by August 30, 1999. The OIS does not plan to develop a continuity plan specifically for PCS and COTS. Rather, PCS and COTS will be incorporated into continuity plans being prepared by the Tier 2 business process owners.

### 4. Trade Database

The Director, OIS; Chief, Information Systems Division, OIS; Senior Database Manager, OIS; Trade and Tariff Information Manager, Office of Operation; and Database Manager, OIS were contacted to obtain the status of this system. Roles and responsibilities for Y2K compliance have been assigned. An inventory of Trade Database components has been developed, but spot checks revealed that it is not complete. OIS personnel have renovated the hardware and software identified in the inventory for Y2K compliance, with the exception of client software used for administration which is planned to be purchased. OIS personnel have reviewed all Trade Database source code to ensure it complies with the manufacturers' specifications to ensure Y2K compliance. Notification to non-Commission users of the Trade Database will take place as part of the External Communications Continuity Plan planned for development by the Office of External Relations. The OIS does not plan to develop a continuity plan specifically for the Trade Database. Rather, the services provided by the Trade Database will be incorporated into continuity plans being prepared by the Tier 2 business process owners.

### 5. Electronic Document Imaging System

The Chief, Information Systems Division, OIS and Computer Specialist, OIS were contacted to obtain the status of this system. OIS personnel have developed an inventory of electronic document imaging system (EDIS) components, and identified the activities necessary to achieve Y2K compliance. Some components can not be renovated to achieve Y2K compliance, although OIS personnel predict that these components will not fail. Many of components for which Y2K remedies are available have not yet been renovated, but OIS personnel plan to start renovation soon and complete renovation by August 1, 1999. OIS is in the process of contracting for a requirements study in order to accelerate plans for EDIS replacement, although a replacement system will not likely be in place prior to January 2000. OIS does not plan to develop a continuity plan specifically for EDIS. Rather, the services provided by EDIS will be incorporated into continuity plans being prepared by the Tier 2 business process owners.

## 6. Electronic Publishing System

The Director, Office of Publishing and Information Systems Specialist were contacted to obtain the status of this system. Significant progress has been made since the initial review. PUB has completed renovation of all hardware and software associated with the Electronic Publishing System (EPS). Key components of the electronic publishing system have been tested by the manufacturer or independent organizations, and have been certified to be Y2K compliant. PUB plans to develop a continuity plan specifically for the EPS.

---

*“Key components of the electronic publishing system have been tested by the manufacturer or independent organizations, and have been certified to be Y2K compliant.”*

---

## 7. PRISM

The Senior Contract Specialist, AD was contacted to obtain the status of this system. The Office of the Director of Administration (AD) personnel have obtained a letter from the PRISM vendor certifying the Y2K compliance of PRISM software. OIS personnel renovated PRISM hardware to achieve Y2K compliance. AD personnel will use manual methods to perform PRISM functions in the event of failure of the PRISM system.

## 8. Building Infrastructure

The Director, Office of Facilities Management (FM) was contacted to obtain the status of this system. Personnel have developed a matrix checklist indicating roles and responsibilities for Y2K compliance, and have obtained manufacturer certifications of Y2K compliance for all building infrastructure components. FM personnel continue to work with General Service Administration and Boston Properties, the building manager, to ensure the availability and safety of the building. FM personnel have begun to develop a contingency plan for the building infrastructure, including building security, and have identified additional resources that will be needed to implement the contingency plan from December 31, 1999 – January 9, 2000.

## VI. CONCLUSIONS

---

*“A spot check revealed that some items which should be identified and tracked for Y2K compliance were not included in the current inventory listing.”*

---

1. The Commission should continually update the inventory of systems and components susceptible to the Y2K problem. OIS and other personnel responsible for Y2K compliance need a certain amount of lead time to complete renovation work. In the event items are identified late, there may be insufficient time to complete renovation and contingency planning.
2. The Commission should continue to update the Commission Action Plan as necessary. The current Action Plan should be used by Y2K Committee to measure actual progress versus planned progress on tasks in order to drive action parties to closure and more accurately predict when major Y2K-related efforts will be completed.
3. The Commission should continue to develop contingency plans for first tier and second tier functions. The Y2K Committee should ensure that mission critical systems continuity plans are properly incorporated in first tier and second tier contingency plans.



U.S. International Trade Commission

# Year-2000 Action Plan

July 2, 1999

## Strategy

Virtually all of the Commission's systems are commercial, off-the-shelf systems. Thus, our situation is unlike that of agencies with custom-built computer systems and their own programmers. The Commission must rely on the vendors of our commercial systems for fixes and assurances of Y2K-compatibility; whether the vendors truly can guarantee compatibility is largely beyond the Commission's control.<sup>1</sup> The Commission's remediation effort focuses on applying the "patches" or upgrades recommended and provided by vendors. The Commission is well along in applying vendor-recommended upgrades and patches. All PCs and almost all network hardware are already upgraded. The Commission has developed an inventory of all vulnerable systems, that has been cross-checked for completeness by a survey of all offices. Commission staff are working their way down this list in rough priority order.

Our assessment of the risk is that the Commission will likely experience some disruption during the first few weeks of January 2000. If public services outside the Commission's control (e.g., power, telephone systems) do not fail, the expectation is that most internal systems can be working within a week, with the likelihood that a few systems will have to be replaced or require extensive work lasting up to a month. The Commission is developing and will use business continuity (contingency) plans, which will involve manual or other work-arounds, to deliver, or if appropriate delay, critical work products until problems can be fixed.

The Commission has considered whether taking additional steps would guarantee Y2K compliance. The Commission could hire contractors to perform extensive system testing. However, that course of action would likely be extremely disruptive to current operations, very expensive, and in the end would not guarantee compliance.<sup>2</sup> Currently, additional funding for Y2K remediation is not anticipated.

---

<sup>1</sup> One aspect of this is that vendors of some key software products have only very recently issued Y2K-compliant versions. This is one reason that remediation efforts are expected to run right up to the last minute.

<sup>2</sup> For example, to fully test a complex system might typically require full-scale simulation of the Y2K date changeover. Should there be a problem that crashes the system, current work would be interrupted, unless substantial, additional funds were provided to operate a fully redundant operational system during the test or perform all testing outside work hours.

## Organization of this plan

This plan is organized generally along the lines of the General Accounting Office's guidelines for Y2K planning, *Year 2000 Computing Crisis: An Assessment Guide* (GAO/AIMD-10.1.14)(GAO Assessment Guide) , which defines 5 phases of remediation:

- Awareness
- Assessment
- Renovation
- Validation, and
- Implementation.

Based on the already-approved High-level Business-Continuity and Contingency Plan (BCCP), this plan also begins to specifically formulate a management-level BCCP. This planning is necessary because many processes depend on internal or external Y2K-vulnerable system that may fail in January, 2000, in spite of our best remediation efforts. The GAO-recommended format for this planning has been followed.

Finally, this plan specifically incorporates a master schedule of Y2K-related events and an inventory of Y2K-vulnerable systems has been incorporated by reference.

## Assignment of responsibilities

By memorandum CO71-W-006 of January 27, 1999, the Chairman assigned the Director of Operations (Director) as the Commission's Y2K Official with overall responsibility for Y2K planning and remediation. The Director is assisted by a Y2K Committee that includes representatives of organizations with major Y2K responsibilities—particularly the Office of Operations' Office of Information Services and the Office of Administration—as well as of the General Counsel, the Inspector General and the Office of External Relations.

The Director is responsible for biweekly Y2K status reporting to the Chairman, as well as quarterly follow-up reporting for the IG's Y2K audit recommendations, and periodic reporting to the Office of Management and Budget.

The Director is also responsible for obtaining budgetary and resource support for Y2K remediation as necessary, and for leading the education and awareness effort among Commission employees.

The Director assigned a working group to conduct a program-office survey to assess Y2K vulnerabilities and business priorities (see below), and has established a biweekly meeting schedule (alternate Tuesdays) for the Y2K Committee.

The Office of Information Services (OIS) is generally responsible for developing systems inventories and for remediation work for Commission information systems (excluding Publishing); the Office of Administration is responsible for those functions with respect to building services, out-sourced personnel, payroll and accounting systems, and Publishing information systems.

The Director of External Relations is responsible for organizing contacts, facilitating cooperative agreements, and communications with outside customers, Congressional oversight and funding committees, business partners, and the public concerning all aspects of Y2K planning and impact.

Office Directors are responsible for making information and resources required for assessment and remediation efforts available to the Director and the Y2K Committee. Office Directors are also responsible for making sure their staffs are aware of Y2K issues that may affect them, and that they follow any Y2K-related guidance issued by the Director.

**Business-process managers<sup>3</sup> are responsible for assessing the criticality of each of their operations' deliverables to customers, and, where necessary, for forming BCCP teams to develop and test plans for continuation of operations, in the event that one or more systems fail (contingency planning).**

## **Y2K remediation planning**

The following topics track the steps recommended in the GAO Assessment Guide. The advice provided in the GAO Assessment Guide was tailored to the Commission's needs because the guide contains a comprehensive list of tasks which are intended to cover the full range of diverse Federal agency systems. Specifically, the guidance was tailored to the Commission's environment of: small scale of operations; no large-scale "customized" systems; and relatively small impact on the public of short-term (one month or less) interruption of one or more of our operations.

---

<sup>3</sup> Business process managers are the lead officials for the Commission's five Strategic Plan operations, plus the critical processes identified as "Tier 1" priorities in the section below on contingency planning.

## Y2K problem awareness

The awareness program within the Commission comprises the following elements:

- *Define the Year-2000 problem and its potential impact on the Commission. This step is complete in the form of the Inspector General's Report Evaluation of the Commission's Preparations for the Year 2000 Report No. IG-3-99(IG Y2K Report 03-99) and associated program management responses.*
- *Designation of the Y2K Official and formation of a Y2K Committee representing key technical and management executives throughout the Commission. This step is complete.*
- *Meet with all Commission managers to brief them on the nature of the problem, outline Commission plans for remediation, review their critical mission requirements, risks and priorities, and discuss alternatives for coping with the problem. The all-managers meeting took place in March, 1999; the office-by-office impact survey was conducted during March and April, 1999.*
- Brief this plan to the IRM Steering Committee and the Budget Committee. Modify plan in light of comments received. This process will be completed by July 9, 1999.
- Advise Commission managers and staff of likely impact of Y2K remediation decisions on their operations. This information will be based on evaluation of the business-impact material gathered in the manager survey, combined with technical assessment of the costs and prospects for replacement or renovation of relevant Y2K-vulnerable systems, alternatives for alternative processing or work-arounds like rescheduling, and Commission-wide priority ranking of remediation projects. The responsibility for this process is with the BCCP Communications Team (to be formed), and the target for completion of this process is September, 1999.
- Advise outside customers, suppliers and other business partners of the impact on service delivery or other change in Commission business practice, schedules, etc. contemplated as a result of Y2K remediation. The responsibility for this process is with the BCCP Communications Team, and the target for completion of this process is tentatively October, 1999.
- Communicate to all Commission staff the plans and guidance for changes in procedures that are planned as part of Y2K remediation, and communicate to managers contingency plans for business continuation in the event of unanticipated or uncontrollable (external) failures of Y2K-vulnerable systems. This process will be the responsibility of BCCP Teams and will occur from November, 1999 through February, 2000, as required.

### **Assessment of vulnerable systems and business risks**

Commission IT and administrative services staff have been working for some time to renovate or replace Y2K-vulnerable systems that are obviously critical to Commission operation, like desktop PCs, ITC-Net servers and networking devices, and the telephone system. Progress on these systems is reflected in the systems inventory attached to this plan, in the IG Y2K Report 03-99, and in Commission reports to Federal oversight agencies. As of June, 1999, remediation on well over 90 percent of systems has been completed.

To assure that other systems that are important to the Commission's mission are identified and targeted for priority remediation, a survey of all offices was conducted in April, 1999, and a few systems were added that were initially missed in earlier inventories.

The complete inventory of systems has been reviewed and a Y2K status assigned to each item. The status is either "Compliant" (remediated) or "Noncompliant." For each noncompliant item, a renovation date has been assigned, or it has been classified as "To be abandoned" or "Low priority" (meaning it may be abandoned without serious consequence if it fails in 2000.)

The total number of noncompliant items as of June 18, 1999, was 45, with 21 of those scheduled for remediation (i.e., not to be abandoned or "low priority"). Only 5 items are scheduled to be renovated after July 31, 1999, and of those, only 1—the Treasury Electronic Certification System operated by Finance & Budget—is a critical system.

### **Renovation of vulnerable systems**

"Renovation" means fixing, replacement or retirement of systems. The Commission has been renovating systems for over a year, based on common-sense priorities and the systems previously identified as "mission-critical" for purposes of security planning.<sup>4</sup> Basic infrastructure and widely used applications were identified as priorities, so the Commission has been working with vendors to fix, upgrade or replace the obvious systems prior to doing a complete analysis of priorities. For example, network file and print servers were upgraded to Y2K-compliant versions of Banyan VINES, an upgrade to a Y2K compliant version of our main desktop application (WordPerfect) was completed, and all individual PC's were made compliant.

---

<sup>4</sup> EDIS and the "ITCNet" were previously identified as critical systems for security planning purposes. "ITCNet" comprises the basic computer infrastructure of network connections, servers, printers, and individual PC's, as well as the Internet connection including the firewall. It does not, however, include any of the applications supported by this infrastructure, like word processing, databases, spreadsheets, e-mail, Internet access, T&A processing, etc., many of which clearly are crucial to Commission operations. The Commission has been reporting to OMB and GSA on this definition of "mission critical systems", though this was modified in the latest (February, 1999) report to include the Tariff & Trade DataWeb and the DOI T&A system, in light of the IG's recent audit recommendations. However, a broader definition of "mission-critical systems" is needed, based on input from Commission business managers on what systems support their "critical" deliverables.

Even for the obviously important systems, however, a significant impediment to renovation has been and continues to be the slowness of delivery by our vendors and suppliers of fixed product versions or software “patches.” For example, a stable version of Microsoft Windows NT Server software, on which several other systems depend, including our Internet firewall, our Lotus Notes applications (including the Sunset information page and the Intranet), and our main Internet Web page (<http://www.usitc.gov>) is still unavailable. The expectation is that required upgrades will be forthcoming soon, but all delays may add to the “year-end rush.”

Principal outside services vendors have been contacted, like PEPCO (electrical power), Bell Atlantic (telephone and local-service access to the Internet), and the Department of the Interior (personnel, payroll and accounting systems.) They have responded with varying degrees of assurance that they will be able to provide continuous service. Where there is less than a full commitment to continued service, it is difficult to estimate how much is real uncertainty and how much is legal hedging. Obviously, planning has incorporated scenarios in which some or all of these services are interrupted.

To provide more specific and timely guidance on renovation, the Commission’s master schedule showing target completion dates for each system is maintained on the Intranet. Here Commission employees can monitor progress on items they depend on.

### **Validation (testing)**

Both Government and private-sector sources indicate that thorough testing of systems to assure Y2K compliance is costly, complex and time-consuming. The Gartner Group, a leading IT consultancy, estimates that seventy percent of all Y2K compliance expense can be consumed in testing. The GAO suggests that some agencies may need “over a year to adequately validate and test converted or replaced mission-critical systems.” They also suggest that “in some instances, agencies may not be able to shut down their production systems for testing, and may thus have to operate parallel [duplicate] systems . . .”<sup>5</sup>

There are no current plans to conduct extensive testing, as this would likely be extremely disruptive to current operations, very expensive, and in the end would not guarantee compliance. In addition, where other agencies may need more extensive testing in part because their systems are unique and highly customized, with programming code developed by the agency itself, or with contractor support, the Commission does not have this same need. Such systems will typically take a long time to fix, so the risk is greater that an outage in January, 2000, would be an extended one. Furthermore, if an agency is the only user of a system, it bears the full burden of locating and repairing the problem. In contrast, virtually all of the Commission’s systems are “off-the-shelf”, mainstream commercial products. The vendors are doing the testing, and if the systems do fail next January, contacts with their many customers will let them quickly find all

---

<sup>5</sup> GAO/AIMD-10.1.14, p. 16.

variations of any problems, and fix them. For users of commercial products, therefore, the need for testing is less.

Notwithstanding the above, some basic “roll-forward” testing was conducted of our PC configurations. Once BCCP Teams have focused on the systems that they are relying on for contingency operations to deliver Tier-1 and Tier-2 products and services, additional testing may be performed.

### **Implementation**

The GAO Assessment Guide lists implementation as a step separate from renovation and testing (validation) because of the assumption that Y2K-compliant systems will be developed and tested “off-line” (in isolation from the regular production environment.) Implementation is the step of integrating the renovated, tested systems back into the rest of the operational network. At the Commission Y2K-updated systems have been continuously implemented as part of the renovation process. The upgraded network servers are in production, as are renovated desktop PCs. DataWeb components have been updated in pieces as software “patches” have become available. Thus, there is no need for any separate implementation phase in the Commission’s remediation plan.

### **Business continuity and contingency planning**

Business-continuity or contingency planning (hereinafter “contingency planning”) is planning for delivering critical Commission outputs to customers if information systems fail *in spite of* remediation efforts, or if *external business partner systems* on which critical Commission outputs depend fail, or if *public infrastructure systems—power, transportation and the like—fail*. The aim of contingency planning is to “safeguard an agency’s ability to produce a *minimum acceptable level* of outputs and services in the event of failures of internal or external mission-critical information systems and services.”<sup>6</sup> (Emphasis in the original.)

The General Accounting Office has provided a model for contingency planning in its *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD-10.1.19.) As with their remediation guidance, this model “provides a conceptual framework for helping *large* agencies to manage the risk of potential Year 2000-induced failures . . .” (Emphasis added.) This guidance will thus be considerably adjusted to fit the Commission’s environment. The first adjustment is that this plan combines both remediation and contingency planning in a single document, and the Y2K Committee will manage both processes.

---

<sup>6</sup> GAO/AIMD-10.1.19, at p.1.

It is important to emphasize that, even more than for remediation planning, contingency planning *can only be done* by managers and domain experts familiar with the critical business processes, and not by technical and support staff. This means, for example, that contingency planning for Title VII investigations must be led by the Director of Investigations, with significant insights from other offices that are directly involved and the staff most experienced with these proceedings.

GAO defines four phases of contingency planning:

- **Initiation.**—Includes establishing a work group, developing a high-level plan and master schedule, identifying critical business outputs, and obtaining executive support;
- **Business impact analysis.**—Defining various Year-2000 failure scenarios, identify detailed dependencies on internal external systems for each critical output process, and define minimum acceptable levels of output for each critical process;
- **Contingency planning.**—Includes making and documenting a separate plan for each critical output, defining event “triggers” that will activate the plan, and establishing a business resumption team and roles for each process; and
- **Testing.**—Includes developing and documenting test plans, preparing and executing tests against major disaster scenarios, and updating plans to correct problems uncovered.

This Plan covers only the Initiation phase of our contingency planning, since the other phases will be conducted by project teams responsible for producing the identified critical business outputs. The plans developed by the project teams will be added to this document (as separate attachments) at the end of each phase (identified in the master schedule, below).

### **Initiation**

For the Commission’s environment, the key “deliverables” of this phase of contingency planning are (1) identifying critical Commission outputs, and (2) for each such output, assigning a team to be responsible for contingency planning for the related process.

The Y2K Committee has conducted its analysis of critical outputs, and forwarded a recommendation to the Chairman on May 24, 1999 in OP-W-022 (available for viewing on the Intranet). The Chairman approved the recommendation on May 25.

This High-Level BCCP identified some functions that must operate during any potential disruption or the Commission may face serious adverse consequences. Those functions, called “first tier functions,” are: (1) building security, (2) remediation of Y2K problems, (3) basic communications, and (4) payroll.<sup>7</sup> Building security would include the protection of the physical plant, the Commission’s personnel, and the Commission’s information resources. The basic

---

<sup>7</sup> The numbers do not indicate priority among the four items, as each is viewed as of primary importance.



communication plan would primarily involve informing employees about whether they should come to work and about other matters of concern, but it would also involve assisting customers (especially those with urgent needs, such as a Senator asking for data or a judge for pleadings, under a tight deadline) and informing them about the status of the Commission's proceedings.

The "second tier" of functions includes the investigation and research activities that fulfill the Commission's mission. Second tier planning will address Commission operations as they are set out in the Strategic Plan: import injury investigations, intellectual property-based import investigations, research program, trade information services, and trade policy support. Those functions are crucial to the Commission's long-term operations, but during January 2000 potentially could be postponed in the event of a massive disruption such as that resulting from a loss of building power or water for an extended period. Proceedings subject to statutory deadlines that the statute does not explicitly allow to be extended are distinguishable in terms of urgency from those that are not so subject, as the entities (courts, Congressional committees, etc.) that impose deadlines in the latter proceedings may be approached for extensions of time. However, for the purposes of contingency planning, both types of proceedings are viewed as appropriate for inclusion in tier two. The plan does not specify a third tier; any activities other than those in the first and second tiers will not require any formal contingency plan within the basic parameters.

Once functions have been prioritized as described above, the next step is conducting contingency planning. With respect to the functions in the first tier, planning will essentially consist of finding a way to perform them even if disruption precluded use of the Commission building.

Contingency planning for the second tier functions is likely to be more elaborate. Because the possible disruption could take several forms (e.g., the Commission could have power but no telephones, or personal computers (PCs) but no network), contingency planning will take into account a variety of scenarios based on different levels of disruption, and lead to plans that address the steps to take if faced with each scenario. The scenarios include: (1) the Commission has no power and/or water, thus precluding use of the building; (2) the Commission has power, water, and PCs, but no network, communications (telephones, facsimile, E-mail), or duplication capability (copiers, Docutech); and (3) the Commission has power, PCs, copiers, and the network (including internal E-mail), but no external communications (telephones, Internet, facsimile, external E-mail).

BCCP team leaders for the identified "Tier 1" (most critical) and "Tier 2" (critical) functions have been identified and were tasked on June 28 with conducting the remaining phases of contingency planning. As shown in the master schedule, the Y2K committee will review documents developed by the BCCP team leaders at the end of each phase. At the end of the final phase the Y2K committee will approve the BCCP final plans. These documents will then be added to the Action Plan as an attachment. Deadlines associated with the contingency planning process are highlighted in the master schedule. The team leaders associated with each function are listed below.

Inspection Report IG-05-99  
Appendix A

<b>Function (Tier)</b>	<b>BCCP team leader</b>
Building security (1)	Director of Administration
Remediation of Y2K problems (1)	Director, Office of Information Services
Basic communications (1)	Director, Office of External Relations
Payroll (1)	Director of Administration
Import injury investigations (2)	Director, Office of Investigations
Intellectual property-based investigations (2)	Director, Office of Unfair Import Investigations
Research program (2)	Director, Office of Industries
Trade information services (2)	Director, Office of Tariff Affairs and Trade Agreements
Trade policy support (2)	Director, Office of External Relations

**Master schedule of Y2K-related events**

<b>Date<sup>1</sup></b>	<b>Event</b>	<b>Responsibility</b>	<b>Status</b>
1/27/1999	Chairman assigns Director of Operations overall responsibility for Y2K planning and remediation (CO71-W-006)	Chairman	Completed
2/23/1999	First biweekly status report to the Commission (OP-W-010)	Rogowsky	Completed
2/25/1999	OMB Quarterly Status Report	Rogowsky	Completed
3/1/1999	Y2K Project Team ("Y2K Committee") formed (first meeting held)	Rogowsky	Completed
3/3/1999	Biweekly status report to the Commission (OP-W-016, 3/5/1999)	Smith (for Rogowsky)	Completed
3/10/1999	"Y2K Awareness" meeting of all Commission managers as a group	Spencer/Olsavsky (for Rogowsky)	Completed

Inspection Report IG-05-99  
Appendix A

<b>Date <sup>1</sup></b>	<b>Event</b>	<b>Responsibility</b>	<b>Status</b>
3/16/1999	Biweekly status report to the Commission (OP-W-014)	Rogowsky	Completed
4/2/1999	Biweekly status report to the Commission (OP-W-017a)	Rogowsky	Completed
4/9/1999	<b>Compilation of survey of all Commission managers to identify critical business processes and their dependencies on Y2K-vulnerable systems</b>	<b>Spencer/Richards</b>	<b>Completed</b>
4/16/1999	Biweekly status report to the Commission (OP-W-017b)	Rogowsky	Completed
5/3/1999	Biweekly status report to the Commission (OP-W-018)	Rogowsky	Completed
5/11/1999	<b>Identify core business processes (BCCP 1.3)</b>	<b>Y2K Committee</b>	<b>Completed (Y2K meeting)</b>
5/17/1999	<b>OMB Quarterly Status Report</b>	<b>Rogowsky</b>	<b>Completed</b>
5/17/1999	Biweekly status report to the Commission (OP-W-021)	Rogowsky	Completed
5/24/1999	<b>Y2K Committee proposal for remediation and contingency planning strategy to Chairman, indicating business risks associated with recommended approach.</b>	<b>Rogowsky, Y2K Committee</b>	<b>Completed (OP-W-022)</b>
5/25/1999	<b>Agency Head accepts risks associated with proposed Y2K Committee remediation plans</b>	<b>Chairman (Rogowsky/Bardos)</b>	<b>Completed</b>
6/1/1999	<b>Complete inventory of Y2K vulnerable systems with remediation status and dates</b>	<b>Director, Information Services</b>	<b>Completed</b>
6/2/1999	<b>Inventory and Commission strategy posted on USITC Intranet and staff requested to review and comment</b>	<b>Director, Information Services</b>	<b>Completed</b>

<b>Date <sup>1</sup></b>	<b>Event</b>	<b>Responsibility</b>	<b>Status</b>
6/1/1999	Biweekly status report to the Commission	Rogowsky	Completed
<b>6/15/1999</b>	<b>BCCP “high-level plan” due to OMB per OMB 99-16</b>	Rogowsky	<b>Completed</b>
6/15/1999	Biweekly status report to the Commission	Rogowsky	Completed
<b>6/28/1999</b>	<b>Contingency planning meeting to assign team leaders of core business processes and task them with BCCP. (BCCP 1.4)</b>	Rogowsky	<b>Completed</b>
<b>6/28/1999 - 7/23/1999</b>	<b>Conduct and document BCCP Business Impact Analysis (BCCP 2.0)</b>	BCCP Team Leaders	
<b>6/30/1999</b>	<b>Status report on IG-03-99</b>	Rogowsky	<b>Completed</b>
6/30/1999	Biweekly status report to the Commission	Rogowsky	Completed
7/1/1999	Status report on remediation progress (systems not yet remediated)	Olsavsky	
7/2/1999	Action plan approved by Y2K Committee	Rogowsky	
7/9/1999	Overall Y2K Plan briefed to IRM/SC and Budget Committee, and published to the Intranet	Rogowsky (Smith)	
7/15/1999	Biweekly status report to the Commission	Rogowsky	
<b>7/30/1999</b>	<b>Review and provide feedback to Team Leaders on Business Impact Analyses</b>	<b>Y2K Committee</b>	
8/4/1999	Biweekly status report to the Commission	Rogowsky	
<b>8/2/1999</b>	<b>Status report on remediation progress (systems not yet remediated)</b>	<b>Olsavsky</b>	

<b>Date <sup>1</sup></b>	<b>Event</b>	<b>Responsibility</b>	<b>Status</b>
8/2/1999 - 8/27/1999	<b>Conduct and document Contingency Planning (BCCP 3.0)</b>	BCCP Team Leaders	
8/15/1999	<b>OMB Quarterly Status Report</b>	Rogowsky	
8/18/1999	Biweekly status report to the Commission	Rogowsky	
9/1/1999	Biweekly status report to the Commission	Rogowsky	
9/1/1999	<b>Completion of all remediation activities</b>	Olsavsky	
9/3/1999	<b>Review and provide feedback to Team Leaders on Contingency Plans</b>	Y2K Committee	
9/6/1999 - 10/1/1999	<b>Conduct and document BCCP Testing (BCCP 4.0)</b>	BCCP Team Leaders	
9/15/1999	Biweekly status report to the Commission	Rogowsky	
10/1/1999	Biweekly status report to the Commission	Rogowsky	
10/1/1999	<b>IG-03-99 Closure Memorandum</b>	Rogowsky	
10/2/1999	<b>Y2K Committee approves BCCP final plans</b>	Rogowsky	
10/15/1999	Biweekly status report to the Commission	Rogowsky	
11/1/1999 - 11/30/1999	<b>BCCP leader for “Basic Communications” communicates with customers, business partners, and staff regarding Y2K impact forecast</b>	Leahy	
11/1/1999	Biweekly status report to the Commission	Rogowsky	
11/15/99	<b>OMB Quarterly Status Report</b>	Rogowsky	
11/15/1999	Biweekly status report to the Commission	Rogowsky	

<b>Date<sup>1</sup></b>	<b>Event</b>	<b>Responsibility</b>	<b>Status</b>
12/1/1999	Biweekly status report to the Commission	Rogowsky	
12/15/1999	Biweekly status report to the Commission	Rogowsky	
1/4/2000	Biweekly status report to the Commission	Rogowsky	
1/19/2000	Final <sup>2</sup> Biweekly status report to the Chairman	Rogowsky	

<sup>1</sup> Deadline for deliverables.  
<sup>2</sup> If warranted, the work of the Y2K committee and the biweekly status reports will continue beyond this date.

**Inventory of Y2K-vulnerable systems posted on the USITC Intranet**