December 15, 1998

MEMORANDUM FOR VAN ZECK, COMMISSIONER
BUREAU OF THE PUBLIC DEBT

FROM: David C. Williams
Inspector General

SUBJECT: Year 2000 Compliance Effort at the Bureau of the Public Debt

This memorandum presents the results of our assessment of the Bureau of the Public Debt's (BPD) Year 2000 conversion effort. We performed a limited review of this effort. In addition to the BPD, the Office of Inspector General (OIG) evaluated and reported on the Year 2000 efforts at other Treasury bureaus individually, as well as from a Department-wide perspective. Subsequent work may be performed by us in the future and will be reported to you in a separate report.

Overall, we concluded that the BPD established an infrastructure for managing its conversion effort and minimizing the risk that a Year 2000 induced failure would have on its mission critical operations. No significant reportable issues came to our attention. Therefore, a formal response to our draft report was not required or provided by the BPD.

However, the inherent nature of the Year 2000 dilemma denies the ability to completely eliminate risk. The Year 2000 problem comes with inherent risks that all organizations face and will continue to face, despite their best efforts and demonstrated success. Accordingly, we developed three suggestions encouraging organizations to sustain their efforts in the areas of change management, data exchange, and contingency planning for business continuity to minimize potential disruptions caused by these inherent risks.

OBJECTIVES, SCOPE, AND METHODOLOGY

The overall objective of our review was to evaluate the BPD's internal Year 2000 conversion effort for its mission critical information technology (IT) systems. Our specific objectives were to evaluate the following: (1) project management; (2) system conversion and certification; and (3) contingency planning for business continuity. In addition, we performed a limited review of the BPD's Year 2000 strategy and progress for non-IT and telecommunications systems.

Our review was limited to evaluating strengths and weaknesses in the management of the Year 2000 conversion project. Specifically, we determined if processes existed and were designed to mitigate the Year 2000 risk to an acceptable level for ensuring all mission critical IT systems remain operable. Therefore, this memorandum is not intended to represent or convey statements that any given system is Year 2000 compliant or that a system will or will not work into the next millennium.

From June through August 1998, using a risk based audit approach, we reviewed and evaluated applicable Year 2000 documentation, including: Treasury's Year 2000 Vulnerability Assessment Report, dated October 1997; the BPD's monthly status reports; the BPD's Year 2000 Project Plan; and other related documents. In addition, we interviewed the appropriate officials within the BPD.

AUDIT RESULTS

Overall, we concluded that the BPD established an infrastructure for managing its conversion effort and minimizing the risk that a Year 2000 induced failure would have on its mission critical operations. The BPD's project management and strategies for conversion, testing, and contingency planning were adequate to address their needs. As a result, no significant reportable issues came to our attention. However, we made three suggestions which may assist the BPD in sustaining their Year 2000 efforts. Details on the results of our assessment and suggestions are provided below.

Project Management

The BPD recognized the Year 2000 issues early, and has continued to demonstrate a high level of awareness and dedication to their Year 2000 conversion effort. Of the five mission critical IT systems at the BPD, four have been implemented and certified with the final system scheduled for implementation March 1999.

System Conversion and Certification Process

The BPD developed and implemented four of its five mission critical systems in the early 1990's which enabled them to initially design the systems to be Year 2000 compliant. This left one mission critical system, which will be replaced by March 1999. The BPD personnel are developing the replacement system and will be performing Year 2000 testing and certification. The BPD historically used in - house personnel to develop, operate, and maintain its systems. As a result, the institutional knowledge has contributed to the success of their Year 2000 efforts. Although the BPD demonstrated a reliable conversion process, we want to emphasize the importance of conversion and testing integrity issues that should be considered as the BPD completes the validation and implementation phases.

Ensuring Year 2000 Conversion Integrity

It is important for the BPD to ensure that subsequent modifications and environmental changes do not nullify certified test results. Generally, the risk that a system may fail due to system changes increases as January 1, 2000 approaches and the time available for additional testing decreases. The risk associated with modifying a system will vary depending on the timing and complexity of the changes. The closer system changes occur to the end of testing and certification, the higher the risk. Additionally, the more applications, programs, and interfaces affected by a specific change, the higher the risk to the conversion and testing integrity. As organizations complete system, integration, and end to end testing, the likelihood increases that even small changes subsequent to these tests could jeopardize the integrity of certification. Business users and management both have critical roles for managing the risk of system changes. They both need to evaluate potential changes in the context of Year 2000 compliance, and balance the risk to operations of not implementing a change with the risk of rendering a system non-Year 2000 compliant.

One suggested practice to mitigate conversion risk is to adopt "freeze policies," or, as done by the Federal Reserve, put in place a "limitation window and moratorium policy[1]." Whether an organization opts for a complete restriction or limited restriction, it is critical that the timing of such a policy is driven by test schedules and progress. The more systems that are tested and certified as Year 2000 compliant, or the more aggressive the existing test schedule is, the lower the tolerance should be for approving changes.

Suggestion

1. We suggest that the BPD Commissioner ensures that a disciplined change management process is in place to maintain Year 2000 conversion integrity. Once a system has been certified, steps need to be taken to ensure system integrity is maintained. Subsequent changes, including platform upgrades, software enhancements, or any system modification should be evaluated and approved with the understanding of the implications. This could be accomplished by establishing specific criteria for approving system changes. Criteria should address such factors as: nature, timing, and extent of requested change; documented assessment of requested change; extent of retesting required; and number of organizations and partners affected.

[1] Terms adopted from the Federal Reserve's century date change management policy. The limitation window is the period where there is a higher standard for requesting and approving system changes. A moratorium would occur towards the end of the limitation window, closer to January 1, 2000, and would further restrict changes.

Coordinating Pivots Dates With Data Exchange Partners

Notable efforts at the BPD include their thorough efforts in managing its interface inventory and coordinating with their data exchange partners. The BPD regularly meets with its main exchange partners, and has successfully tested many of the interfaces. Through regular contact, the BPD and the Federal Reserve agreed to use the same pivot dates to better ensure the successful exchange of data. In fact, this example of excellent coordination between partners provided the basis for the following suggestion being reported to all the bureaus.

For exchange partners using a windowing logic technique in lieu of a four digit field expansion, special care needs to be given to coordinate pivots.[2] For example, all Treasury bureaus exchange payroll, budget, and accounting data with the National Finance Center and the Financial Management Service, both of which use the windowing logic technique. If exchange partners choose different pivots, the century identifiers could be incorrectly inferred if further processing, calculating, or sorting is performed on data transferred. For example, if the BPD is using a pivot date of 50 and its exchange partner is using a pivot date of 60, date values in between 1950 through 1960 and 2049 through 2059 could be calculated in error. Without coordination with exchange partners, bureaus may not adequately develop and test new data exchange formats, nor apply the necessary bridges and filters to ensure the exchanges will function properly. The greater the number and complexity of data exchanges, the greater the challenge in identifying, synchronizing, and testing exchange formats.

Suggestion

2. We suggest that the BPD Commissioner ensures data exchange procedures include the identification and coordination of pivot dates with its exchange partners. Where there are differences in pivot dates, the BPD should ensure that filters are installed to synchronize and maintain the accuracy of century identifiers. This is especially important between processing partners, i.e., those partners whose data is transferred for further processing.

[2] The windowing logic technique uses pivots to interpret a two digit year into a four digit year. All year values above the pivot are understood to represent one century; while all values below the pivot are understood to represent another century. Pivots refer to a number built into system logic to infer the 2 digit century identifier “19” or “20”. For example, a pivot of 50 infers 19 as the century identifier for values 50-99 and infers 20 for values 0-49.

Contingency Plans for Business Continuity

The BPD prepared short term contingency plans for each of its mission critical systems. The individual plans outline procedures to cover the period of time needed to take corrective action. The BPD also prepared an overall, more long term continuity plan that will be closely coordinated with their Disaster Recovery Plan. Although they have developed a strategy that meets the needs of their organization, we want to reiterate the importance of contingency planning and issues that should be considered when developing contingency plans.

It is management's responsibility to reduce the risk of Year 2000 related failures and maintain a minimum acceptable level of service. Contingency planning is required to assure continuity of operations in the event of an unanticipated Year 2000 failure, and for systems that will not be Year 2000 compliant. Contingency planning should address risks not only with internal systems, but external risks with business partners and the public infrastructure. Plans should identify resources, procedures, and appropriate training required to carry out core business functions. Plans should clearly identify triggers for implementation, be tested thoroughly, and continuously reevaluated. Steps should be included that facilitate the restoration of normal services at the earliest possible time.

Suggestion

3. We suggest that the BPD Commissioner ensures that management prioritizes and facilitates the preparation and testing of contingency plans for each core business function, as well as mission critical information systems. As part of managing the development and potential implementation of these plans, management should ensure that: these plans consider both the internal and external risks; resources and implementation triggers are identified; training in executing the plan is performed; and the plans are periodically evaluated for reasonableness.

We appreciate the courtesies and cooperation provided to our auditors during the audit. If you wish to discuss this report, you may contact me at (202) 622-1090 or a member of your staff may contact Barry L. Savill, Director of Audit at (202) 283-0151.

cc: Treasury Departmental Offices
Assistant Secretary for Management and Chief Financial Officer
Deputy Assistant Secretary for Information Systems
and Chief Information Officer
Assistant Director of Information Technology Policy and Management
Director, Office of Organizational Improvement
Director, Office of Strategic Planning
Director, Financial Management

Office of Budget
Office of Accounting and Internal Control
Management and Controls Branch

Bureau of the Public Debt
Noel Keesor, Assistant Commissioner, Office of Information Technology

Office of Management and Budget
Michael S. Crowley, Budget Examiner

YEAR 2000 COMPLIANCE EFFORT
AT THE
BUREAU OF THE PUBLIC DEBT

OIG-99-020 **DECEMBER 15, 1998**

Office of Inspector General

****

United States Department of the Treasury