THE YEAR 2000 COMPLIANCE EFFORT
AT THE
UNITED STATES SECRET SERVICE

OIG-99-024 DECEMBER 21, 1998

Office of Inspector General

****

United States Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON

INSPECTOR GENERAL

December 21, 1998

MEMORANDUM FOR LEWIS C. MERLETTI, DIRECTOR
UNITED STATES SECRET SERVICE

FROM: for David C. Williams Richard B. Calahan
Inspector General

SUBJECT: Year 2000 Compliance Effort at the United States Secret Service

This memorandum presents the results of our assessment of the United States Secret Service's (Secret Service) Year 2000 conversion effort. We performed a limited review of this effort. In addition to the Secret Service, 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 Secret Service 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 Secret Service.

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 the Secret Service, as well as other Treasury bureaus, to sustain 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

Our overall objective was to evaluate Secret Service's 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 plans for business continuity. In addition, we performed a limited review of Secret Service'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 September 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; Secret Service's monthly status reports; Secret Service's Year 2000 Project Plan; and other related documents. In addition, we interviewed the appropriate officials within the Year 2000 IT Working Group and Non-IT Working Group who had responsibilities for the Year 2000 effort, as well as the Year 2000 Bureau Executive and Assistant Year 2000 Bureau Executive.

This audit was conducted in accordance with Government Auditing Standards issued by the Comptroller General of the United States, and included such audit tests as were deemed necessary.

AUDIT RESULTS

Overall, we concluded that the Secret Service 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. Secret Service's project management and strategies for conversion, testing, and contingency planning were adequate to address their needs. No significant reportable issues came to our attention. However, we made three suggestions which may assist the Secret Service, as well as other bureaus, in sustaining their Year 2000 efforts. Details on the results of our assessment and suggestions are provided below.

Project Management

We concluded that Secret Service established an effective project management foundation to address Year 2000 issues. Senior management and staff were knowledgeable of Year 2000 issues and committed to the successful continuation of operations into the next century. Secret Service's success can be attributed to the Year 2000 established working groups that included both information system personnel along with business owners. IT and non-IT working groups were established to aid in managing and focusing the Year 2000 conversion effort. These working groups were further supplemented by subgroups tasked with targeted issues and concerns.

System Conversion and Certification Process

Secret Service's Year 2000 conversion and testing strategy was adequate to minimize the occurrence of potential Year 2000 related failures. As of September 1998, Secret Service had tested and implemented 14 of 18 mission critical systems. Secret Service anticipated that the remaining four mission critical systems are scheduled for implementation by February 1999. Secret Service has not had any major schedule slippage, nor do they anticipate any difficulty or significant delay in converting, testing, or implementing all its systems.

Secret Service's Year 2000 conversion and testing strategy uses a combination of repair and replacement techniques. Those systems being repaired will undergo field expansion to accommodate a four digit century. After the systems are repaired, testing will be done in three phases: (1) unit testing; (2) system testing; and (3) Year 2000 certification testing. The Year 2000 certification testing, which is testing the integration of all systems, cannot begin until all applications are corrected. Date rollover tests will be incorporated in the Year 2000 certification testing. Secret Service anticipated certification testing to begin December 1998 with completion scheduled for April 1999.

Secret Service's certification test plan is designed to validate date fields and date dependent program logic. Secret Service will conduct Year 2000 certification testing in a logical partition. This environment will contain Year 2000 compliant system software, converted Year 2000 databases, and compliant application systems. Prior to undergoing Year 2000 certification testing, all applications will have been converted, tested, and implemented.

Ensuring Year 2000 Conversion Integrity

It is important for Secret Service 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 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 Secret Service Director ensures 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 test 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.

Coordinating Pivots With Data Exchange Partners

We determined that Secret Service developed a reasonable plan to address data exchange issues. Secret Service identified external interfaces for data exchange, obtained agreements with all its data exchange partners, and developed bridge programs to convert incoming and outgoing dates to conform to its internal eight-character date standard. Secret Service would have the ability to take corrective action quickly for any unforeseen problems with its data exchange.

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

[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.

[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.

inferred if further processing, calculating, or sorting is performed on data transferred. For example, if Secret Service 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 Secret Service Director ensures data exchange procedures include the identification and coordination of pivot dates with its exchange partners. Where there are differences in pivot dates, Secret Service 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.

Contingency Plans For Business Continuity

Based on our interviews, we concluded that Secret Service is committed to preparing contingency plans to ensure continuous operations into the next century. As of September 1998, draft contingency plans had been prepared for most of Secret Service's mainframe applications. However, these plans had not been reviewed by management, and therefore were not available for our review. In addition, Secret Service was in the process of developing a business continuity plan. Secret Service plans to use the end of 1998 and all of 1999 to continuously refine these plans. Although Secret Service has 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 Secret Service Director ensures the continued development, testing, and reevaluation of contingency plans for each core business function, as well as mission critical 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 review. 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 Division
Office of Budget
Desk Officer, Management and Controls Branch
Desk Officer, Office of Accounting and Internal Control

United States Secret Service
Stephen Colo, Chief Information Officer and Bureau Year 2000 Executive
Ron Thomsen, Assistant Year 2000 Bureau Executive
Ken Gunderson, Assistant Chief Computer Support
John Best, Senior Program Manager, Office of Administration
James W. Burke, Special Agent in Charge

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