INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

November 21, 2003

MEMORANDUM FOR CHIEF INFORMATION OFFICER

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Assistant Inspector General for Audit (Small Business and Corporate Programs)

SUBJECT: Office of Audit Comment Concerning Management's Response to the Audit Report, *Risks Are Mounting as the Integrated Financial System Project Team Strives to Meet an Aggressive Implementation Date* (Audit # 200320038)

The subject audit report was issued in draft on August 25, 2003. At the request of the Business Systems Modernization Office (BSMO), we provided an extension of time for you to provide your response and comments to the draft report. Since we did not receive a response by the extension due date of October 2, 2003, we released the final report without a response. In a memorandum dated October 21, 2003, your office provided a response to the report that agreed with six recommendations and disagreed with one recommendation.

Your office agreed that the disaster recovery environment for the Integrated Financial System (IFS) would not be optimal or fully tested before initial implementation and provided corrective actions to ensure that the disaster recovery environment is completely built out and tested as soon as possible. However, your office disagreed that the IFS disaster recovery classification in the draft Technical Contingency Planning Document be reconsidered.

Disaster Recovery Will Not Be Optimal or Fully Tested Before Initial Implementation

The Technical Contingency Planning Document is required to describe business contingency capabilities for a system before the system is implemented. The final IFS Contingency Plan was not available prior to the completion of our audit fieldwork. However, we reviewed the draft Contingency Plan and noted that the IFS was classified as a "critical" system. We believe the Internal Revenue Service (IRS) should reconsider classifying this system as "mission critical" for two reasons.[1]

First, the IFS supports 3 of the 18 mission critical business processes, as defined in the IRS Business Contingency Case For Action. Second, the definition of "critical" in the draft Contingency Plan may not fit the IFS. The draft Contingency Plan states that a "critical" system:

- Is critical in accomplishing the work of the IRS.
- Is primarily performed by computers.
- Can be performed manually for a limited time period.

Based on our analysis and discussions with BSMO officials, it would be very difficult to perform the full range of IFS capabilities manually for a limited time period. Because the Contingency Plan was still in draft, we did not determine why the system was classified as "critical" versus "mission critical." However, confusion seems to stem from the definition of critical infrastructure[2] versus the classification definitions in the draft Technical Contingency Planning Document. If the IFS is not classified correctly, plans may not be made to recover the system in time to perform mission critical tasks.

To ensure that a high-quality system is delivered, we recommended that the CIO ensure the IFS classification in the draft Technical Contingency Planning Document is reconsidered.

Management's Response: Your office did not concur with this recommendation and stated that it was understood that the recommendation was made to ensure that IFS receives a higher consideration when planning for disaster recovery. However, IFS is not a system critical to the IRS core mission. The current IFS disaster plan encompasses using the Enterprise Integration and Test Environment (EITE) resources at Martinsburg Computing Center (MCC) to partially recover IFS. The modernization disaster recovery planning for 2004 and 2005 will provide enough business functionality for the IRS to stay in business in the event of a site disaster.

Office of Audit Comment: Your office's response states that the IFS is not a system critical to the IRS core mission. However, the IRS has determined that it has 18 mission critical processes, as defined in its Business Contingency Case For Action, and

[1] A "critical" system must be restored within 5 days, or 120 hours, after a disaster. A "mission critical" system must be restored within 36 hours after a disaster.

[2] Presidential Decision Directive 63, *Critical Infrastructure Protection*, requires agencies to identify and protect critical infrastructures (physical and cyber-based systems) that are essential to the minimum operations of the economy and Federal Government.

that the IFS will support 3 of these 18 mission critical processes. In addition, your office states that modernization disaster recovery planning for 2004 and 2005 will provide enough business functionality for the IRS to stay in business in the event of a site disaster. In response to an earlier recommendation in the report, your office stated that IFS disaster recovery planning is in its early stages. As a result, we cannot comment fully on 2004 and 2005 disaster recovery planning. Therefore, our opinion remains that the IFS classification may need to be reconsidered as a mission critical system for disaster recovery purposes.

While we still believe our recommendation is worthwhile, we do not intend to elevate our disagreement concerning IFS disaster recovery classification to the Department of the Treasury for resolution. Consequently, no further action on your part is required.

Please contact me at (202) 622-6510 if you have questions, or your staff may call Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

cc: Associate Commissioner, Business Systems Modernization