DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

JUL 25 2003

MEMORANDUM FOR TONI L. ZIMMERMANN, CHIEF
INFORMATION TECHNOLOGY SERVICES
M:I

FROM: Mary V. Ronan for
CHARLENE WRIGHT THOMAS
ACTING PRIVACY ADVOCATE CL:PA

SUBJECT: Computing Systems Software and Operations Privacy Impact Assessment (PIA)

The Office of the Privacy Advocate has reviewed the Privacy Impact Assessment for the Computing Systems Software and Operations (CSSO) system. Based on the information you provided, we do not have any privacy concerns that would preclude this system from operating. However, a revised PIA is required when considering any future upgrades or major modifications to the system or before the project progresses to the next milestone.

We will forward a copy of the PIA to the Director, Security Services Mission Assurance Certification Program Office to be included in the Security Accreditation Package for formal acceptance for operation. The Director, Security Policy Support and Oversight, which has security oversight responsibility, may request information concerning the statements contained in the PIA to ascertain compliance with applicable requirements.

If you have any questions please contact me at 202-927-5170; or your staff may contact Priscilla Hopkins at 202-927-9758.

Attachment

cc: Director, Security Services Mission Assurance, Certification Program
Office M:S:A
Director, Security Policy Support and Oversight M:S:S
Division Information Officer Pamela Carlson IS:S

(DRAFT - 6/12/02)

Date

MEMORANDUM FOR CHARLENE W. THOMAS
ACTING PRIVACY ADVOCATE CL:PA

FROM: TONI L. ZIMMERMANN, CHIEF
INFORMATION TECHNOLOGY SERVICES
M:I

SUBJECT: Request for Privacy Impact Assessment (PIA) –
Computing Systems Software and Operations (CSSO)

Purpose of the System:
Computing Systems Software and Operations (CSSO) is the mainframe and server data processing infrastructure, and the people who operate and maintain it. It includes the physical computers and peripherals, with the system software, and the operations staff. The business applications run on our infrastructure, and their programs are scheduled and started by our people. In the course of performing these functions, it creates, collects, and uses administrative data that assists in properly configuring the mainframes and servers, and controlling their operation.

Name of Request Contact:
Name: Chris Siple
Organization Name & Symbols: M:I:EO:OR
Mailing Address: A6-278 NCFB
Phone Number (with area code): 202-283-3528

Name of Business System Owner:
Name: Toni L. Zimmerman/Jeffrey Cooper
Organization Name & Symbols: M:I:EO
Mailing Address: B4-401 NCFB
Phone Number (with area code): 202-283-0990

Requested Operational Date: Systems are operational.

Category: *(Reason PIA is required--enter "y" or "n" and applicable dates)*
New System?: __n__ (CSSO is not a new system, but it has never been assessed)
Recertification? (if no change, enter date of last certification) ____n____
Modification of existing system?: ___n___
Is this a National Standard Application (NSA)?: ___n___
Is this a Modernization Project or System? ___n___
If yes, the current milestone?: __5__ *(Enter 1-5; explain if combining milestones)*

System of Record Number(s) (SORN) #: *(coordination is required with Office of Disclosure--contact David Silverman, 202-622-3607)*

After reviewing our PIA request, that office has confirmed that "the Privacy Act does not require an SOR" for CSSO because it is "machinery/computer architecture".

Attachment: PIA

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories: A. Taxpayer B. Employee C. Audit Trail Information (including employee log-in info) D. Other (Describe)	(Most of the data that is housed physically on the equipment we maintain is not defined, collected, read, or used by us. All taxpayer data is controlled by the business applications and is covered in their PIAs. We create, collect, and use administrative data that assists us in properly configuring the mainframes and servers, and controlling their operation.) D. Service level agreement (SLA) data that lists the outputs expected by our customer and tracks its timeliness; system software configuration parameters; capacity management data that assists us in capacity planning.
2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources. A. IRS B. Taxpayer C. Employee D. Other Federal Agencies (List agency) E. State and Local Agencies (List agency) F. Other third party sources (Describe)	All the data we define, collect, read, or use is obtained from the IRS. It is developed by our own employees, gleaned from negotiations with our customers, or collected from internal computer system performance monitors.
3. Is each data item required for the business purpose of the system? Explain.	Yes. This data allows us to operate and maintain the infrastructure according to the requirements of our customers..
4. How will each data item be verified for accuracy, timeliness, and completeness?	SLAs are negotiated with our customer and tracking data is verified by their actual experience. Configuration parameters are verified through the testing process on the test partitions and systems. Capacity data is verified by matching it with actual computer performance.
5. Is there another source for the data? Explain how that source is or is not used.	There is no other source for the data.
6. Generally, how will data be retrieved by the user?	SLA data is read from system consoles in the form of scheduling messages and output tracking reports. Configuration parameters is read from terminals by our system programmers. Capacity management data is either read on terminals or is printed in reports.
7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?	No, it is not. This data concerns only the performance of the machines we operate and the jobs that run on them.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?	Schedulers, System software specialists, and capacity management experts will have access to this data.
9. How is access to the data by a user determined and by whom?	Managers decide whether the schedulers etc. need to access/update which data.
10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared. If NO, continue to Question 12.	No.
11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?	na
12. Will other agencies provide, receive, or share data in any form with this system?	No.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?	Tapes are scratched and written over; DASD files are deleted.
14. Will this system use technology in a new way? If "YES" describe. If "NO" go to Question 15.	No.
15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.	No.
16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.	No. .
17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently? Explain.	No.
18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?	na
19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?	na