



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

RECEIVED  
04 APR 26 AM 7:27  
OFFICE OF DISCLOSURE  
OP-EX-GLD:0

APR 02 2004

MEMORANDUM FOR DARIUS TAYLOR  
DIRECTOR, DEVELOPMENT SERVICES

FROM: Maya A. Bernstein *Maya A. Bernstein*  
Privacy Advocate

SUBJECT: Windows Server 2003 (w/o Active Directory)  
Privacy Impact Assessment

The Office of the Privacy Advocate has reviewed the Privacy Impact Assessment (PIA) for the Windows Server 2003 (w/o Active Directory). Based on the information you provided, our office does not have any privacy concerns that would preclude the Windows Server 2003 (w/o Active Directory) from operating. However, before the system is designated as a platform for IRS business data use, an updated PIA is required.

We will forward a copy of the memo and PIA to the Director, Modernization and System Security, to be included in the formal package for this system. That office may request information concerning the statements contained in the PIA to ascertain compliance with applicable security requirements.

In accordance with the E-Government Act of 2002, this PIA may be posted on the IRS.Gov web page. A copy of this PIA will be forwarded to the Office of Disclosure for their review.

If you have any questions, please contact me at 202-927-5170 or Gino Talbot at 202-622-2302

Attachment

cc: Director, Regulatory Compliance  
Director, Office of Disclosure

March 24, 2004

MEMORANDUM FOR MAYA A. BERNSTEIN  
PRIVACY ADVOCATE

FROM: Peggy Gladwell, Chief Technical Section, End-User Equipment and Services (EUES), OS:CIO:I:EU:TS

SUBJECT: Request for Privacy Impact Assessment (PIA) –  
*Windows Server 2003 (w/o Active Directory)*

Purpose of the System: The purpose of the *Windows Server 2003* system is to provide the basic server operating system architecture so that applications that process sensitive but unclassified (SBU) data can operate and communicate effectively. There is no SBU data on this system at this time. A new and updated PIA will be supplied when data is introduced into this system.

Name of Request Contact:

Name: Peggy Gladwell

Organization Name & Symbols: Technical Services (OS:CIO:I:EU:TS)

Mailing Address: 312 Elm Street  
Suite 2200

Cincinnati, OH 45202

Phone Number (with area code): 859-669-5529

Name of Business System Owner:

Name: Al Whitley

Organization Name & Symbols: End-User Equipment & Services (OS:CIO:I:EU)

Mailing Address: New Carrollton Federal Building  
5000 Ellin Road

Lanham, MD 20706

Phone Number (with area code): 202-283-0864

Requested Operational Date: June 2004

Category: (Reason PIA is required--enter "y" or "n" and applicable dates)

New System?: no

Recertification? (if no change, enter date of last certification) no

Modification of existing system?: no

Is this a National Standard Application (NSA)?: no

Is this a Modernization Project or System? no

If yes, the current milestone?: \_\_\_\_\_ (Enter 1-5; explain if combining milestones)

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

**Data in the System**

<p>1. Describe the information (data elements and fields) available in the system in the following categories:</p> <ul style="list-style-type: none"> <li>A. Taxpayer</li> <li>B. Employee</li> <li>C. Audit Trail Information (including employee log-in info)</li> <li>D. Other (Describe)</li> </ul>	<p>The Windows Server 2003 system doesn't process data; it is an operating system. However, certain employee data is used to create network login accounts that enable employees to access the system. This data is limited to the data gathered when the employee completes a Form 5081. This data includes first initial, the middle initial (or X if there is no middle name), first 4 characters of the user's last name, and the user's district office code. While Windows Server 2003 does harvest and store audit trail data, it isn't used to process that data.</p>
<p>2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.</p> <ul style="list-style-type: none"> <li>A. IRS</li> <li>B. Taxpayer</li> <li>C. Employee</li> <li>D. Other Federal Agencies (List agency)</li> <li>E. State and Local Agencies (List agency)</li> <li>F. Other third party sources (Describe)</li> </ul>	<p>N/A</p>
<p>3. Is each data item required for the business purpose of the system? Explain.</p>	<p>N/A</p>
<p>4. How will each data item be verified for accuracy, timeliness, and completeness?</p>	<p>N/A</p>
<p>5. Is there another source for the data? Explain how that source is or is not used.</p>	<p>No.</p>

<p>6. Generally, how will data be retrieved by the user?</p>	<p>The user will know there is a discrepancy if they are unable to logon. Users are granted appropriate access rights to their home directory, shared data folders or applications as required and approved by their management through the use of a Form 5081.</p>
<p>7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?</p>	<p>No</p>

Access to the Data

<p>8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?</p>	<p>Users, Managers, Administrators, and Developers will have access to the Operating System to setup, test, and develop the system for eventual use</p>
<p>9. How is access to the data by a user determined and by whom?</p>	<p>The only data directly used by the server is the user's name and all users have the ability to determine that information.</p> <p>The Domain Administrators for a Windows Server 2003 server define the rights and access levels of the users. Users are granted permission to their own directory and to any other shared directories, applications, or files specified by the users' managers on the Form 5081.</p>
<p>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.</p>	<p>N/A</p>
<p>11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?</p>	<p>N/A</p>
<p>12. Will other agencies provide, receive, or share data in any form with this system?</p>	<p>N/A</p>

Administrative Controls of Data

<p>13. What are the procedures for eliminating the data at the end of the retention period?</p>	<p>The operating system's only data is comprised of user login information. When employees leave the service, user accounts are deleted and proper documentation is maintained for 6 years in case it's needed as a result of an internal inquiry.</p>
<p>14. Will this system use technology in a new way? If "YES" describe. If "NO" go to Question 15.</p>	<p>No.</p>
<p>15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.</p>	<p>No.</p>
<p>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.</p>	<p>Yes. As stated in LEM 25.10.8.7.2.1, Auditing and Incident Response Security Standards:</p>
<p>17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently? Explain.</p>	<p>No.</p>
<p>18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?</p>	<p>N/A</p>

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?	N/A
--	-----