




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

JUN 22 2004

MEMORANDUM FOR FRANK KIST DIRECTOR, ENTERPRISE NETWORKS

FROM: Maya A. Bernstein  
Privacy Advocate 

SUBJECT: Enterprise Remote Access Project  
Privacy Impact Assessment

The Office of the Privacy Advocate has reviewed the Privacy Impact Assessment (PIA) for the Enterprise Remote Access Project (ERAP) System. Based on the information you provided, our office does not have any privacy concerns that would preclude ERAP from operating. A revised PIA is required when considering any major modifications to the ERAP system, or at the scheduled recertification of this system/application.

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

Note that the Electronic Government Act of 2002 requires that the IRS make this PIA available to the public. If there is any portion of this PIA that you believe would cause harm to the IRS or any party if disclosed to the public, please mark those portions and return to our office within 10 days.

If you have any questions or would like to discuss this PIA, please contact me at 202-927-5170. Our staff analyst is Gino Talbot at 202-622-2302.

Attachment

cc: Director of Regulatory Compliance

May 19, 2004

MEMORANDUM FOR MAYA A. BERNSTEIN  
PRIVACY ADVOCATE

FROM: Frank Kist, Director, Enterprise Network, OS:CIO:I:EN

SUBJECT: Request for Privacy Impact Assessment (PIA) – Enterprise Remote  
Access Project (ERAP)

Purpose of the System: The Enterprise Remote Access Project Virtual Private Network was designed by AT&T for the IRS in order to provide a secure network transport solution for taxpayer support. ERAP will provide connectivity for IRS' remote sites to the IRS Data Centers using VPN technology. ERAP will support normal IRS business operations by providing access to standard networked IRS enterprise applications and resources.

The ERAP VPN solution will support multiple types of remote sites. AT&T and the IRS have defined the following primary location types:

- IRS fixed sites – Locations owned by the IRS, however without direct IRS network access.
- Non-IRS fixed sites – Locations potentially owned and managed by other non-IRS entities, but providing IRS related function or support.
- Home – Static locations, which are permanent domestic dwellings, occupied by an IRS employee(s) requiring remote IRS network resource access.
- Mobile – A location that has neither been identified as fixed site of IRS business or a domestic dwelling, yet the IRS employee(s) require remote IRS network resource access.

Name of Request Contact:

Roger Newlin  
Enterprise Network, OS:CIO:I:EN:M:C  
5000 Ellin Road B4-358  
Lanham MD. 20706202-283-6472

Name of Business System Owner:

Frank Kist  
OS:CIO:I:EN  
5000 Ellin Road B5-100  
Lanham MD. 20706  
202-283-5748

Privacy Impact Assessment – Enterprise Remote Access Project (ERAP)

Requested Operational Date:

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

New System?:   y  

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?:        *(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)*

Treasury/IRS 00.001 – Correspondence Files & Correspondence Control Files.

Attachment: PIA

**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>ERAP is a secure transport medium that carries data from one location to another. ERAP does not process or store data. The data types transported by ERAP vary from sensitive taxpayer data, emails, application data, or personal employee data such as social security numbers. The only data known to temporarily reside within the ERAP VPN will be the operational system event logs.</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>The ERAP will not store, process or retain end-user data. The only data that reside within the ERAP VPN will be the operational system event logs. These system logs will be captured by the IRS Enterprise Management Center's (EMC) management tools and ticketing system. The captured information will be used for the purposes of system alerting and maintenance and considered sensitive but unclassified (SBU)</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>The ERAP is a VPN transport system that uses [REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>ERAP uses the [REDACTED]</p> <p>[REDACTED]</p> <p>ensure accuracy and completeness. The ERAP VPN performs checks from end to end. When user data is submitted into the VPN, [REDACTED]</p> <p>[REDACTED]</p> <p>Timeliness is ensured via the Service Level Agreement.</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>Using their assigned VPN Account the user has to establish a VPN session. The user then logs on to IRS network to access their data. Users only have access to data or applications as 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>Yes.</p> <p>After a user is logged into the IRS system via a Secure VPN session the transfer of SBU data is possible for normal day-to-day IRS business activity.</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>User will only have access to data or application as approved by their management through the use of a Form 5081. Managers and system administrators have access to each ERAP devices to setup, test and maintain availability of ERAP.</p>
<p>9. How is access to the data by a user determined and by whom?</p>	<p>Users only have access to data or applications as approved by their management through the use of a 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>No.</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>No.</p>

**Administrative Controls of Data**

<p>13. What are the procedures for eliminating the data at the end of the retention period?</p>	<p>User login accounts used by the system to authenticate users are disabled when employees leave or are terminated, and are the only information kept in the system. The system login information is kept for the length of the contract with AT&amp;T.</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>No.</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>
<p>19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?</p>	<p>N/A</p>