



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

FEB 05 2004

MEMORANDUM FOR KEN HOCKENBERRY
DIRECTOR, WORKLOAD MANAGEMENT BRANCH

FROM: Maya A. Bernstein
Privacy Advocate

A handwritten signature in black ink, appearing to read "Maya A. Bernstein".

SUBJECT: Secure Drop Box Sun Server
Privacy Impact Assessment

The Office of the Privacy Advocate has reviewed the Privacy Impact Assessment (PIA) for the Secure Drop Box Sun Server (SDBSS). Based on the information you provided, our office does not have any privacy concerns that would preclude Secure Drop Box Sun Server from operating.

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 for operation. That office may request information concerning the statements contained in the PIA to ascertain compliance with applicable security requirements. If you have any questions, please contact me at 202-927-5170; or Gino Talbot at 202-622-2302.

CC: George Jakabcin Director, Modernization and System Security
Rose Hernandez Director, Regulatory Compliance

Privacy Impact Assessment – Secure Drop Box Sun Server (SDBSS)

Title of System: Secure Drop Box Sun Server (SDBSS)

Is this a new system, or an existing system? This is a new system that will reside in the XXXXXXXX Common Communication Gateway (CCG).

If an existing system is this submission because of: (circle)

Modification

Re-certification with no-change

Modernization project

If this PIA is for a modernization project, circle the milestone:

One

Two

Three

Four

Final implementation

List all Systems of Records Notices (SORNs) under which this system operates. (Provide documentation from Headquarters Disclosure Office)

The Disclosure Office concurs that the SDBSS will operate under this SORN.

Treasury/IRS 30.003 Requests for Printed Materials Including Lists.

Name, Title, Mailing Address of System Owner:

Ken Hockenberry
Director Workload Management Branch
5000 Ellin Road
Lanham, MD 20706

System Owner's Operating/Functional Division: OS:CIO:I:EO:OR:WM

PIA Preparer/email/phone: Paul J. Biro/Paul.J.Biro@irs.gov/202-283-3529

Subject matter contact/email/phone:

Paul J. Biro/Paul.J.Biro@irs.gov/202-283-3529

Introduction

The Toll-Free effort of the ADC Outsourcing A-76 project is a process that will use a Sun XXXXX Server as a secure Drop Box to route incoming and outgoing files to/from Alpine Access to the IRS XXXXXXXX Computing Center (XXX). This Drop Box server will be part of the Common Communication Gateway (CCG) infrastructure housed in XXX .

The Drop Box will be connected to the Internet using the public WAN and administering external file transfers via an XXXXXXXXXXXXXXXX. The IPsec VPN Tunnel is to be set up by Telecommunication in XXX and XXXXX. Files coming in from Alpine Access (SBU Files) will come through the IPsec VPN Tunnel, run through XXXXXXXXXXXXXXXXXXXX, 'dropped' in their designed IP address 'portal' on the Drop Box. Once the dropped file(s) are authenticated and approved by internal IRS systems, then the files are sent via FTP to the Centralized Inventory Distribution System (CIDS) Mainframe housed in XXX.

The files that are transmitted by Alpine Access as part of the Toll-Free effort will be authenticated and authorized through the use of the Enterprise FTP Network Server (EFNS) housed in XXX. XXX personnel will need to develop a script to create the work order files to be sent to/from the Drop Box to/from EFNS as well as the CIDS mainframe. The files are to be sent electronically to Alpine Access through the secure Drop Box scheduled once daily XXXXXX Eastern Time (ET) Monday – Saturday. Files from Alpine Access will be received by IRS one time daily at XXXXXXXX Sunday – Friday.

The files are initially administered in EFNS through the use of Form 12038 wherein the Director, XXXXXXXX Computing Center will authorize the transfer and receipt of files to/from EFNS. File transfers will be pre-identified by CIDS mainframe SA/DBA and coordinated with the EFTU 12038 Administrator in XXX. All data files transmitted to/from the Drop Box in XXX to/from the CIDS mainframe in XXXXXXXX will need to be installed in the EFTU 12038 database. Data files issued by the CIDS mainframe are considered non-SBU files.

Data file transfers are conducted using File Transfer Protocol (FTP). Data coming in from Alpine Access to the secure Drop Box in XXXXXXXX will be 'Pulled' by EFNS and sent via FTP to the CIDS mainframe. All data transfers from the CIDS mainframe being sent to Alpine Access through the secure Drop Box will be 'Pulled' from CIDS mainframe by the EFNS stored on the EFNS server and forwarded via ftp to the Drop Box. Data files from CIDS are Forms Inventory Update files that contain no T/P ID or pertinent data. The files that we send to Alpine are;

DISK.TEST.PRODUCT.EXTRACT (product and revision information)

DISK.TEST.CENTERP.EXTRACT (center product information including inventory for products by center)

DISK.TEST.OPVARIA.EXTRACT (maximum quantities for taxpayers and practitioners for publications & forms used to check ordered quantities and possibly put order into override status if order exceeds these maximums)

| | |
|--|--|
| <p>1. Describe the information (data elements) available in the system in the following categories. (Provide copy of data dictionary if available.)</p> <ul style="list-style-type: none"> A. Taxpayer B. Employee (including employee log-in info) C. Other (Describe) | <p>For A,B,&C – The server is designed to be a secure pass through system only. Data files that are sent from IRS, Centralized Inventory Distribution System (CIDS) mainframe, are non-SBU files. The CIDS mainframe data files are CIDS Inventory update files that are issued to Alpine Access via the secure drop box Sun server located in XXXXXXXX's Common Communication Gateway. The only employee access to the drop box server will be by designated Systems Administrators from Tier2 for regular schedule maintenance and any downtime of the server. The drop box server has no other users.</p> |
|--|--|

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)

For A,B,C,D,E,F – Only data file indicators will be passed through the EFNS 12038 database. This database will contain – File Name, File Size, File Frequency, File Owner, File Destination, Internet Protocol (IP) address for Internal customers plus the secure drop box server and Password, Time of day file is processed, cycle time, file owner email and phone number, and Point of Contact for error resolution. The password designates the Alpine Access server that is issuing the files to the IRS. There is also a password on the Secure Drop box. It is used for security and server identification purposes. For files issued from Alpine Access it lets the Drop Box know that the files being sent strictly from the server registered for Alpine Access. All files sent in from Alpine Access are sent to the CIDS mainframe via the Enterprise FTP Network Server (EFNS) residing in XXX.

IRS ADC Outsourcing /CIDS mainframe will issue three flat files updated database files to Alpine Access that are subsequently used by calling center personnel employed by National Institute for Severely Handicapped (NISH).

DISK.TEST.PRODUCT.EXTRACT (product and revision information)

DISK.TEST.CENTERP.EXTRACT (center product information including inventory for products by center)

DISK.TEST.OPVARIA.EXTRACT(maximum quantities for taxpayers and practitioners for publications & forms used to check ordered quantities and possibly put order into override status if order exceeds these maximums)

The files are to be sent electronically to Alpine Access through the secure Drop Box scheduled once daily by XXXX. The incoming forms request file(s) from NISH, whose employees take the forms orders from Taxpayers, will be sent to Alpine Access and then batched transmitted from Alpine Access to the XXXXXXXX Internet Gateway eventually going to the CIDS mainframe. The parameters for the NISH Alpine Access files are:

NAME-ADDRESS-CITY-STATE-ZIP/CODE AND PRODUCT REQUESTS.

Data sent from the IRS is non-SBU designated data. Files coming from Alpine Access contain Taxpayer Privacy Act data and are designated as SBU. It is deposited on the Drop Box and forwarded to the CIDS mainframe for scheduled delivery. For specifics regarding the operations of the CIDS Mainframe, please refer to the CIDS PIA.

Privacy Impact Assessment – Secure Drop Box Sun Server (SDBSS)

| | |
|--|---|
| <p>3. Explain why each data item is needed for the business purpose of the system.</p> | <p>Data files that are issued from the CIDS mainframe through the secure drop box Sun server are in support the Toll-Free effort of the ADC Outsourcing A-76 project.</p> <p>Taxpayers will call in all taxpayer form requests through the following three product lines impacted by the direct-transfer of the ADC telephone program to an outside vendor: 1-800-829-3676, 1-800-829-1040 and 1-800-829-4933.</p> <p>The business needs the capability to route calls coming in on the 1-800-829-3676 product line to one of three entities: the ADCs, the NTI/NISH vendor, and designated W&I sites (listed below). Domain Name server (DNIS) 3676 calls routed to the W&I AM sites should be intelligently routed. W&I AM sites may need additional circuitry (as described below) to handle the anticipated volume of calls.</p> <p>The business needs the capability to route those callers selecting "Know the form" in menus to both the ADCs and W&I AM sites.</p> <p>Effective February 2, 2004, the vendor (Alpine Access, contractor for National Telecommuting Institute/National Institute for Severely Handicapped [NTI/NISH]) who will receive the FTEs being outsourced, will need direct database updates from the CIDS systems. This access will be needed for approximately 2 years or until new systems are designed by the winning bidder on the ADC outsourcing contract (either government or private sector).</p> |
| <p>4.a. How will each data item be verified for accuracy, timeliness and completeness?</p> | <p>Data issued from the CIDS mainframe as well as data files received in the drop box will be transmitted to the Enterprise FTP Network Server (EFNS) 12038 database for authentication and authorization. All files sent in from Alpine Access are sent to the CIDS mainframe via the Enterprise FTP Network Server (EFNS) residing in XXX. The information is taken directly from the authoritative source (requester).</p> |
| <p>4.b. Is there another source for the data that is more reliable? Explain why that source is not being used.</p> | <p>NO.</p> |

| | |
|---|---|
| <p>5. How will the data generally be retrieved by the users?</p> | <p>Internal users (CIDS mainframe) will have data files transmitted through the EFNS system residing in XXX that will FTP (PUSH) incoming files from the drop box to CIDS mainframe. All data received from Alpine Access through the XXXXXXXXXXXXXXX and through the XXXXXX Drop Box server will reside on the server no longer than one hour. The flat file containing orders to be batch processed by CIDS will be delivered to the E420R Drop Box by Alpine XXXXXX EST Sunday – Friday. Transfer of data from the Drop Box through the IRS firewall to the IRS WAN will be sent via File Transfer Protocol (FTP).</p> <p>These FTP transfers will be directed through the Enterprise FTP Network Server (EFNS) resident in XXX. An EFNS Work Order script will reside on the Drop Box as well as the CIDS mainframe.</p> <p>EFNS will verify that the data transfers from Alpine Access are authenticated and approved via the 12038 database resident in XXX. A pre-set Work Order script developed for EFNS residing on the Drop Box will send a message to the EFNS Server in XXX. The EFNS server will authenticate and approve the transfer from the Drop Box server per the pre-entered 12038 database. EFNS will then complete an FTP "PULL" command from the drop box. The data file will be stored on the EFNS until such time as the CIDS mainframe is ready to receive the file EFNS will forward the file to the CIDS Mainframe in XXX via an FTP "PUSH".</p> |
| <p>6. Can the data be retrieved by a personal identifier (name, SSN, or other unique identifier)? If yes, explain when it will be retrieved this way.</p> | <p>NO. Files that are sent in from Alpine Access cannot be retrieved through the Drop Box or EFNS. The only authorized personnel that have access to these files are the CIDS personnel that actually fill the form requests.</p> |

Access to the Data

| | |
|---|--|
| <p>7. Who will have access to the data in the system? (Users, Managers, System Administrators, Developers, Other)</p> | <p>Database Administrators will have access. For updating data in the 12038 database. System Administrator for routine maintenance and error resolution.</p> |
|---|--|

Privacy Impact Assessment – Secure Drop Box Sun Server (SDBSS)

| | |
|---|--|
| <p>8. How is user access to the data determined and by whom? Describe the procedures and persons responsible for determining access. Include a description of the process used to determine "need to know" for different categories of users.</p> | <p>The CIDS mainframe data is made up of forms inventory and used for the forms distribution centers. The Toll-Free effort of the ADC Outsourcing A-76 project is the initial phase of the ADC Outsourcing project. CIDS mainframe inventory updates will be sent in a secure manner through the EFNS in XXX to the secure drop box in XXXXXXXX CCG. Data is transmitted from the drop box to an outside vendor Alpine Access. Alpine Access is the secure transfer depository for the incoming forms requests from NTI/NISH and the secure recipient of the CIDS mainframe inventory updates. This first phase of the ADC Outsourcing Project will begin with Forms inquiries made to 800-829-3676.</p> |
| <p>9. 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, Skip to question 12.</p> | <p>There is only one interface system with the secure drop box; and that is the EFNS system in XXX. All data files sent to and received in the drop box will be routed to the EFNS. The question asked for other IRS system interface. Alpine Access will only have the XXXXXXXXXX for access to the Drop box.</p> |
| <p>10. Have the IRS systems described in Item 9 received an approved security certification and approved Privacy Impact Assessment? If yes, provide copies of memoranda.</p> | <p>No. The secure Drop Box is currently going through its certification and accreditation, RIS OPR-4-0004-A00.</p> |
| <p>11. Will other agencies receive data in any form from this system? If yes, provide copy of inter-agency agreement.</p> | <p>No. The data files that are sent/received in the drop box to/from Alpine Access will be solely IRS owned.</p> |

Administrative Controls of Data

| | |
|---|--|
| <p>12. What are the procedures for eliminating the data at the end of the retention period? Cite IRM reference.</p> | <p>Data files sent/received in the secure drop box are retained on the drop box server for no longer than one clock hour. After this time period the files are deleted from the drop box server.</p> |
| <p>13.a. Does this system have new technology?</p> | <p>No. The Drop Box Server is a Tier2 infrastructure Sun XXXXXXXXXXXXXXXXXXXX server.</p> |

Privacy Impact Assessment – Secure Drop Box Sun Server (SDBSS)

| | |
|---|---|
| <p>13.b. How does this new technology affect taxpayer or individual privacy?</p> | <p>No impact on taxpayer or individual privacy.</p> |
| <p>14. Will this system have the capability to identify or locate individuals or groups? If so, describe the business purpose for this capability.</p> | <p>NO. Neither Alpine or EFNS have the capability to allow the specific identification of an individual or group. These two systems will send/receive FTP files only.</p> |
| <p>15. Will this system have the capability to monitor individuals or groups? If so, what controls are in place to prevent unauthorized monitoring?</p> | <p>NO.</p> |
| <p>16. Can use of the system allow IRS to treat taxpayers, employees or others differently? Explain.</p> | <p>NO.</p> |
| <p>17. Can the use of the system allow IRS to make determinations about individuals that would not have been possible otherwise? Explain.</p> | <p>NO.</p> |
| <p>18. Does the system ensure due process by allowing affected parties to respond to any determination that may harm them prior to final action? If yes, explain. If no, explain.</p> | <p>NO. The secure drop box sun server does not retain data files. This drop box server infrastructure is strictly a 'pass-through' system.</p> |
| <p>19. If the system is web-based, does it use persistent cookies or other tracking devices to identify the web visitor?</p> | <p>NO. This system has not web-based interface.</p> |