National Account Profile (NAP) – Privacy Impact Assessment

PIA Approval Date – Jul. 11, 2011

System Overview

The National Account Profile (NAP) is an application used for reconciliation and research to identify discrepancies and help resolve issues. NAP is a compilation of entity data from a number of sources and is provided in a single repository to enhance case worker accuracy and productivity. NAP compiles information, such as individual taxpayer data, business taxpayer data and cross reference data, which is retrieved using a taxpayer identification number (TIN).

Systems of Records Notice (SORN):

- IRS 24.046--Customer Account Data Engine Business Master File
- IRS 24.030--Customer Account Data Engine Individual Master File
- IRS 34.037--IRS Audit Trail and Security Records System
- IRS 42.021--Compliance Returns and Project Files

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer – The NAP contains entity data:
   - Taxpayer Identification Number (TIN)
   - Name
   - Address
   - SSN
   - Employee Identification Number (EIN)
   - Company name
   - Change of address indicator
   - Date the address change was made
   - District/Area Office

B. Audit Trail Information: None contained within the NAP application. Audit trail functionality is provided by the host platform [e.g., Integrated Data Retrieval System (IDRS)]. NAP is an application that is accessed through other applications. Those other applications are responsible for ensuring an appropriate audit trail is maintained.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS – NAP data is obtained from the following master files and TIN assignment files.
   - Individual Master File (IMF)
   - Business Master File (BMF)
   - Employee Plans Master File (EPMF)
   - Individual Taxpayer Information Number (ITIN)

   The systems above have the following data elements:
   - TIN
   - Name

- Address
- SSN
- EIN
- Company name
- Change of address indicator
- Date the address change was made
- District/Area Office

B. State and Local Agencies –The Social Security Administration (SSA) sends to the NAP system the NUMIDENT information which contains Taxpayers' Social Security information included in the following files:
   - Death Master File (DMF)
   - Data Master 1 (DM–1)

3. Is each data item required for the business purpose of the system? Explain.
Yes. The NAP application is designed as an IRS Master File research tool and each data item is required for the business purpose of the system, which is to identify those records for a respective taxpayer so that a filed tax return can be processed correctly.

4. How will each data item be verified for accuracy, timeliness, and completeness?
The NAP application does not manipulate data and only receives and stores data directly from authoritative data stores and is refreshed weekly to remain in sync with master file and SSA data. NAP pulls information from authoritative data sources from various master files. NAP is refreshed weekly to remain in sync with Master File and SSA data. There are no end–users that have direct access to NAP data. Users will access NAP data via IDRS via command code. NAP relies strictly on the authoritative data being input from other systems.

5. Is there another source for the data? Explain how that source is or is not used.
No, there are no other sources from what is mentioned above. NAP is a compilation of entity data from a number of sources and provided in a single repository to enhance case worker accuracy and productivity.

6. Generally, how will data be retrieved by the user?
IRS employees access NAP data through a host platform (e.g. IDRS). The host platform provides authentication and authorization services, as well as audit trail functionality. Users must have an account established with appropriate managerial authorization. Each user's account profile determines what data that user may access, and these permissions are granted on a "need–to–know" basis.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes, NAP data is retrieved for specific taxpayers by TIN.

<u>Access to the Data</u>

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
There are no end users that have direct access to the data within NAP. Only the Modernization & Information Technology Services (MITS)–Enterprise Operations (EOps) System Administrators have direct access to the application data. NAP data is accessed via IDRS via command codes. End–users

have no access to the data within NAP, except for queries via the IDRS system. The users accessing the data via IDRS may be employees or contractors.

9. How is access to the data by a user determined and by whom?
No end users will have direct access to the data stored in NAP. Users access NAP data via another system IDRS through which they will authenticate and use command codes to access the NAP data. They can only view the data via a query within the IDRS system. The access for users is approved by the respective managers of the case workers or other workers requiring access to the NAP application.

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.
Yes, NAP receives SSN and EIN data from the following master files:

- Individual Master File (IMF)
- Business Master File (BMF)
- Employee Plans Master File (EPMF)

TIN assignment files are received from:

- Adopted Taxpayer Identification Number (ATIN)
- Individual Taxpayer Identification Number (ITIN)

The following IRS business systems access NAP to validate the following data:

- Name
- Taxpayer Identification Numbers (TIN)

The systems are as follows:

- Correspondence Letter System (CRX)
- National Change of Address (NCOA)
- Dependent Data Base (DEPDB)

Processing systems:

- Individual Master File (IMF)
- Business Master File (BMF)
- Information Returns Master File (IRMF)
- Federal Tax Deposit (FTD)
- Electronic Filing System – Reference (ELF–R)
- Modernized e–File (MeF)
- Integrated Submission & Remittance Processing (ISRP)
- Generalized Mainline Framework (GMF)
- Electronic Management System (EMS)
- Centralized Authorization File (CAF)
- Weekly TIF Update (WTU)
- Error Resolution System (ERS)
- Electronic Federal Payment Posting System (EFPPS)

Compliance systems:

- Automated Underreporter System (AUR)
- Questionable Refund Project (Part of Electronic Fraud Detection System [QRP])

Online access systems:

- Standardized CFOL Access Protocol (SCAP)
- Standardized CFOL Overnight Processing (SCOP)
- Standardized IDRS Access (SIA)
- Security and Communications System (SACS)
- Integrated Data Retrieval System (IDRS)

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?

Yes. The platforms that provide the processing and storage capabilities for the tax processing systems are tested and certified by the IRS Security Certification Office. In order for each of the individual applications to certified as applications running on a certified platform, they are required to perform a privacy impact assessment.

The following are not FISMA reportable applications. Therefore, it does not have an approved Security Certification and Privacy Impact Assessment.

- National Change of Address (NCOA)
- Standardized CFOL Access Protocol SCAP
- Standardized CFOL Overnight Processing SCOP

Business Master File (BMF)

- Authority to Operate (ATO) – June 14, 2010
- Privacy Impact Assessment (PIA) – March 16, 2010

Individual Master File (IMF) (Subsystem ATIN)

- Authority to Operate (ATO) – March 8, 2010
- Privacy Impact Assessment (PIA) – November 10, 2009

Information Returns Master File (IRMF) (Subsystem of Information Returns Processing (IRP))

- Authority to Operate (ATO) – March 8, 2010
- Privacy Impact Assessment (PIA) – October 9, 2009

Federal Tax Deposit (FTD)

- Authority to Operate (ATO) – May 26, 2009
- Privacy Impact Assessment (PIA) – April 8, 2009

Employee Plans Master File (EPMF)

- Authority to Operate (ATO) – February 5, 2009
- Privacy Impact Assessment (PIA) – November 19, 2008

Individual Taxpayer Identification Number Real–time System (ITIN–RTS)

- Authority to Operate (ATO) – October 1, 2009
- Privacy Impact Assessment (PIA) – February 24, 2009

Dependent Data Base (DEPDB)

- Authority to Operate (ATO) – May 6, 2009
- Privacy Impact Assessment (PIA) – February 20, 2009

Electronic Filing System – Reference (ELF–R)
- Authority to Operate (ATO) – May 26, 2009
- Privacy Impact Assessment (PIA) – April 15, 2009

Modernized e–File (MeF)
- Authority to Operate (ATO) – May 14, 2010
- Privacy Impact Assessment (PIA) – March 29, 2011

Integrated Submission & Remittance Processing (ISRP)
- Authority to Operate (ATO) – February 9, 2009
- Privacy Impact Assessment (PIA) – May 3, 2011

Generalized Mainline Framework (GMF)
- Authority to Operate (ATO) – February 18, 2009
- Privacy Impact Assessment (PIA) – October 16, 2008

Automated Underreporter System (AUR)
- Authority to Operate (ATO) – May 6, 2009
- Privacy Impact Assessment (PIA) – February 27, 2009

Questionable Refund Project (Part of Electronic Fraud Detection System [QRP])
- Authority to Operate (ATO) – June 20, 2008
- Privacy Impact Assessment (PIA) – December 17, 2010

Integrated Data Retrieval System (IDRS)
- Authority to Operate (ATO) – March 10, 2009
- Privacy Impact Assessment (PIA) – November 6, 2008
    - CRX (sub–system)
    - CAF (sub–system)
    - WTU (sub–system)
    - SIA (sub–system)

Electronic Management System (EMS)
- Authority to Operate (ATO) – May 31, 2011
- Privacy Impact Assessment (PIA) – November 19, 2010

Error Resolution System (ERS)
- Authority to Operate (ATO) – May 11, 2009
- Privacy Impact Assessment (PIA) – February 27, 2009

Electronic Federal Payment Posting System (EFPPS)
- Authority to Operate (ATO) – March 19, 2010
- Privacy Impact Assessment (PIA) – January 5, 2010

12. Will other agencies provide, receive, or share data in any form with this system?
Yes, the SSA NUMIDENT database will send weekly update files (Data Master –1, Death Master File) to the IRS Master File System (ECC–DET) via a virtual private network (VPN) tunnel connection. NAP will obtain the data from the Master File System.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
NAP is non–record application, and does not require scheduling. NAP data is a copy of master file data (maintained for 30 years in accordance with IRM 1.15.29, Item 203). As data is added to or deleted from the master files, these changes are reflected in NAP. NAP is updated weekly from its data sources. Those data sources retire data at the end of its retention period. If data is not on the data source, it is not on NAP. The NAP data is continuously overwritten by data received from the master file.

14. Will this system use technology in a new way?
No. NAP does not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
No. NAP is a system which consists of a set of computer programs set to run in a specified order on the IBM Mainframe. It does not allow end users access thus the system cannot be directly used to identify or locate individuals or groups.

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. NAP is a system which consists of a set of computer programs set to run in a specified order on the IBM Mainframe. It does not allow end users access thus the system will not provide the capability monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. NAP is a system which consists of a set of computer programs set to run in a specified order on the IBM Mainframe. It does not allow end users access thus the system does not directly allow the IRS to treat taxpayers, employees, or others, differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Not applicable, NAP is a system which consists of a set of computer programs set to run in a specified order on the IBM Mainframe. It does not allow end users access thus this control is not applicable.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
Not applicable, the NAP system is not web–based thus this control is not applicable.

View other PIAs on IRS.gov