

Business Performance Management System (BPMS) – Privacy Impact Assessment

PIA Approval Date – Dec. 17, 2010

System Overview:

The Business Performance Management System (BPMS) is a “shared service” environment for business intelligence delivery utilizing a data warehouse back–end, including an extraction transformation load ETL layer, with an online front–end capable of planned, scheduled and ad–hoc reporting. BPMS hosts multiple projects that service users throughout the enterprise, providing historical, current, and predictive views of business operations to support improved decision–making and analysis. BPMS utilizes commercial off the shelf (COTS) products, including Microsoft (MS) Structure Query Language (SQL) Server and SAP Business Objects.

Systems of Records Notice (SORN):

- IRS 22.061--Information Returns Transaction File (IRTF)
- IRS 24.030--Individual Master File (IMF)
- IRS 24.046--Business Master File (BMF)
- IRS 26.009--Automated Lien System (ALS)
- IRS 36.001--Appeal, Grievances, and Complaints Records
- IRS 36.003--General Personnel and Payroll Records
- IRS 42.001--Examination Administrative File
- IRS 42.008--Audit Information Management System (AIMS)
- IRS 44.001--Appeals Case Files
- IRS 44.003--Unified System for Time and Appeals Records (UNISTAR)
- IRS 70.001--Statistics of Income (SOI)
- IRS 34.037--IRS Audit Trail and Security Records System

Data in the System

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

- A. Taxpayer – Information provided by existing IRS internal applications and/or subsystems to include taxpayer identification number (TIN) and state of residence.
- B. Employee – Information provided by existing IRS internal applications and/ or subsystems to include standard employee identification number (SEID) and workstation number.
- C. Audit Trail Information – Auditing of the operating system and database occurs but is managed by Modernization Information Technology Services (MITS) Enterprise Operations (EOps). Auditing at the BPMS application level is configured to include a date/timestamp, the unique identifier of the user requesting the information, the action taken, the name of the object modified, the role of the user, and the success or failure of the event. Reports have been created which analyze the data in the auditing files and returns data on users and what reports those users access.
- D. Other – The MIS Data Warehouse contains archived data from existing IRS legacy systems or other existing balanced measures and workload indicator MIS information. This information is neither taxpayer nor employee specific and cannot be considered personally identifiable information (PII).

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

A. IRS:

- BPMS utilizes existing reports or data files generated from a number of existing Tier I, Tier II and Tier III systems. These include: Automated Information Management System – Computer Information System (A-CIS), Automated Substitute for Return (ASFR), Field Assistance Management Information System (FAMIS), Collection Activity Reports (CAR), and Work Planning & Control System (WP&C), MITS Reports, Compliance Data Engine Release 3 (CDEr3), Computer Assisted Review of Error Resolution (CARE), Custodial Detail Database (CDDDB), Treasury Integrated Management Information System (TIMIS), Taxpayer Advocate Management Information System (TAMIS), Systemic Advocacy Management
- System, Release 2 (SAMS II) – These applications collect the following PII data elements:
 - FAMIS
 - Non-standard Employee ID
 - Non-standard Workstation Number
 - Taxpayer Assistance Center (TAC)
 - CDEr3
 - TIN

B. Employee:

- FAMIS
 - Non-standard Employee ID
 - Non-standard Workstation Number
 - Taxpayer Assistance Center (TAC)
 - Login ID from Q-Matic workstation (only first 20 characters are passed)

3. Is each data item required for the business purpose of the system? Explain.

Yes. The data is necessary for the business purposes of the system. The data received depicts all of the functional area Balanced Critical Measures. BPMS enables users to track, monitor, analyze and manage performance data from the IRS Intranet through online access to BPMS.

- Critical Measures
- Weekly / Monthly Performance data
- Division Specific “Tailored Reports”
- Other Supporting Documents for the SP&B / PM Cycle
- Relevant data necessary for management information purposes

4. How will each data item be verified for accuracy, timeliness, and completeness?

The Business Unit supplying the data ensures that the data is valid, accurate, timely and complete. Once approved the information is released to BPMS for posting. BPMS contains extracts from existing IRS legacy systems, each of which have their own internal validation and verification processes. This provides the ability to compare the actual data extract to the data contained in the BPMS for verification when required.

5. Is there another source for the data? Explain how that source is or is not used.

No, there are no other sources of data.

6. Generally, how will data be retrieved by the user?

Data within BPMS is accessed via the Business Objects front–end, which is accessible via the IRS intranet.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?

No, Query retrieval of data by filtering PII elements is blocked by the BPMS application.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

- Each project housed within BPMS has its own domain of users as illustrated below. Users from each project only have access to the project domain that they have been granted access.

Roles: BPMS Standard Users

Permissions: Read, create, and store reports within private application folders (no write access to database)

Roles: BPMS Business Users

Permissions: Create and delete reports assigned to their accounts within the public application folders (no write access to database)

Roles: BPMS Power Users

Permissions: Edit any reports across all application folders (no write access to database)

- The following user roles apply to the entire BPMS application, crossing individual projects.

Roles: BPMS Administrators

Permissions: Read, write, delete reports; Read Data; and modify the application parameters (no write to database)

Roles: Database Administrators

Permissions: Read, write, delete information within BPMS application databases

Roles: System Administrators

Permissions: Modify the operating system parameters on the servers supporting BPMS

Note: Contractors do not have access to the application.

9. How is access to the data by a user determined and by whom?

The IRS Online (OL) 5081 process is utilized to track requests for BPMS access and document the approvals. Two levels of manager approval are required to access BPMS via the web interface. The OL5081 process is also utilized to grant administrator access to the servers, database, and application code. These specialized permissions are only granted when a valid need–to–know is verified.

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.

- Automated Information Management System – Computer Information System (A-CIS)
- Automated Substitute for Return (ASFR)
- Field Assistance Management Information System (FAMIS)
- Collection Activity Reports (CAR)
- Work Planning & Control System (WP&C)
- Modernization & Information Technology Services (MITS) Reports
- Compliance Data Engine Release 3 (CDEr3),
- Computer Assisted Review of Error Resolution (CARE)
- Custodial Detail Database (CDDDB)
- Treasury Integrated Management Information System (TIMIS)
- Taxpayer Advocate Management Information System (TAMIS)
- Systemic Advocacy Management
- System, Release 2 (SAMS II)

BPMS loads available data, using output files, from existing IRS and legacy systems. Additionally, BPMS sends data to Suite of Tools for the Review and Creation of Automated Work-plans and Schedules (STRAWS) and Enterprise Telephone Database (ETD). Neither of these interfaces includes any PII data.

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

The systems listed in item 2 & 10 are certified IRS CPE systems, or are application databases on existing certified systems.

Automated Information Management System – Computer Information System (A-CIS)

- Authority To Operate (ATO) – March 19, 2010
- Privacy Impact Assessment (PIA) – July 24, 2009

Capitalized Asset Management System (CAMS)

- Authority To Operate (ATO) – February 15, 2008
- Privacy Impact Assessment (PIA) – December 17, 2007

Embedded Quality Submission Processing (EQSP)

- Authority To Operate (ATO) – June 16, 2008
- Privacy Impact Assessment (PIA) – May 12, 2008

Automated Substitute for Return (ASFR)

- Authority To Operate (ATO) – June 19, 2008
- Privacy Impact Assessment (PIA) – March 7, 2008

Field Assistance Management Information System (FAMIS)

- Authority To Operate (ATO) – March 27, 2009
- Privacy Impact Assessment (PIA) – March 3, 2009

Federal Unemployment Tax Account (FUTA)

- Authority To Operate (ATO) – December 9, 2009
- Privacy Impact Assessment (PIA) – December 9, 2009

Collection Activity Report (CAR) – component of Integrated Data Retrieval System

- Authority To Operate (ATO) – March 10, 2009
- Privacy Impact Assessment (PIA) – November 6, 2008

Notice Delivery System (NDS)

- Authority To Operate (ATO) – May 3, 2010
- Privacy Impact Assessment (PIA) – March 29, 2010

Combined Annual Wage Reporting (CAWR)

- Authority To Operate (ATO) – June 14, 2007
- Privacy Impact Assessment (PIA) – November 30, 2007

Information Technology Assets Management System (ITAMS)

- Authority To Operate (ATO) – May 22, 2009
- Privacy Impact Assessment (PIA) – April 2, 2009

Taxpayer Advocate Management Information System (TAMIS)

- Authority To Operate (ATO) – June 11, 2009
- Privacy Impact Assessment (PIA) – July 30, 2008

Security Audit and Analysis System (SAAS):

- Authority To Operate (ATO) – June 9, 2010
- Privacy Impact Assessment (PIA) – April 9, 2010

Systemic Advocacy Management System, Release 2 (SAMS II)

- Authority To Operate (ATO) – April 13, 2009
- Privacy Impact Assessment (PIA) – February 20, 2009

Suite of Tools for the Review and Creation of Automated Work-plans and Schedules (STRAWS)

- Authority To Operate (ATO) – March 10, 2010
- Non-FISMA Reportable.

Electronic Transmitted Documents (ETD) – part of Electronic Filing System:

- Authority To Operate (ATO) – May 26, 2009
- Privacy Impact Assessment (PIA) – April 15, 2009

12. Will other agencies provide, receive, or share data in any form with this system?

Yes. The Treasury Inspector General for Tax Administration (TIGTA) has the capability to view data in BPMS upon official request.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?

A request for records disposition authority for the Business Performance Management System and associated records is currently being drafted with the assistance of the IRS Records and Information

Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions for BPMS inputs, system data, outputs and system documentation will be published in IRM 1.15.16, item number to be determined.

14. Will this system use technology in a new way?

No. BPMS does not and will 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. BPMS is not designed to perform this functionality.

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. BPMS will not provide the capability to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?

No. BPMS does not allow IRS to treat taxpayers, employees or others differently. BPMS will not affect the equitable treatment of taxpayers and employees.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

No. BPMS does not ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action, as BPMS does not make negative determinations.

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

No. The web interface does not utilize persistent cookies or other tracking devices to identify web visitors. The MIS Data Warehouse is an internal (Intranet) resource available only within the Treasury Firewall for IRS employees. The Web Interface Business Objects (BOBJ) has the capability to record and audit employee activity via their IRS network login. This is required by auditing regulations.

[View other PIAs on IRS.gov](#)