
A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Business Masterfile Case Creation Nonfiler Identification Process, BMF CCNIP

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Business Masterfile Case Creation Nonfiler Identification Process, BMF CCNIP, #1355

Next, enter the **date** of the most recent PIA. 5/29/2015

Indicate which of the following changes occurred to require this update (check all that apply).

- No Addition of PII
- No Conversions
- No Anonymous to Non-Anonymous
- No Significant System Management Changes
- No Significant Merging with Another System
- No New Access by IRS employees or Members of the Public
- No Addition of Commercial Data / Sources
- No New Interagency Use
- No Internal Flow or Collection

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

- No Vision & Strategy/Milestone 0
- No Project Initiation/Milestone 1
- No Domain Architecture/Milestone 2
- No Preliminary Design/Milestone 3
- No Detailed Design/Milestone 4A
- No System Development/Milestone 4B
- No System Deployment/Milestone 5
- Yes Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

A.1 General Business Purpose

5. What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

The Business Master File Case Creation Nonfiler Identification Process (BMF CCNIP) is an application that creates Selected BMF and Employee Plans Master File (EPMF) Nonfiler tax delinquency cases for the Small Business/Self Employed (SB/SE), Tax Exempt and Government Entities (TEGE), and Large Business and International Division (LB&I) Operating Divisions. BMF CCNIP Project is organizationally driven in support of the SB/SE Key Strategy to increase compliance among SB/SE business taxpayers. BMF CCNIP improves quality and program efficiency by providing a uniform system for selecting cases with the highest potential to satisfy the objectives established by the Business Unit into the Nonfiler treatment stream. Additionally, BMF CCNIP creates an integrated approach to creating Nonfiler cases for business taxpayers similar to the process currently used for individual taxpayers. BMF CCNIP provides access to data sources for Workload Identification, identifying cases for delivery to employees, as well as provides integrated filing compliance performance and management tools. The BMF CCNIP process impacts SB/SE, LB&I and TEGE taxpayers. BMF CCNIP is not a system of record for any taxpayer data. BMF CCNIP has 10 or fewer Analyst users who can update work schedule data and selections and 25 or fewer users who have read only access to reports. All users access BMF CCNIP via the IRS Employee User Portal.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **yes**, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or tax identification numbers (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse Yes On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes Social Security Number (SSN)
Yes Employer Identification Number (EIN)
Yes Individual Taxpayer Identification Number (ITIN)
No Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes Practitioner Tax Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers).

No strategy planned for the application. There is no alternative to the use of the SSN's and EIN's. The SSN's and EIN's are significant parts of the data being processed. The BMF.CCNIP system requires the use of EIN's and SSN's because no other identifier can be used to uniquely identify a taxpayer for intergovernmental communications. There is no known mitigation strategy planned to eliminate the use of SSNs/EINs for the system. The SSN and EIN is required for the use of this system.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	Yes

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
No	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

<u>Yes</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e
<u>Yes</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>No</u>	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
<u>No</u>	PII for personnel administration is 5 USC
<u>No</u>	PII about individuals for Bank Secrecy Act compliance 31 USC
<u>No</u>	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. Explain the detailed business needs and uses for the SBU/PII, and how the SBU/PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The data items are required to identify business non-filers and select them for the return delinquency notice process.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

BMF CCNIP receives data from Integrated Production Model (IPM), which has its own verification process for data accuracy, timeliness, completeness and therefore BMF CCNIP assumes that the data is accurate, timely, and complete when it is provided by IPM.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

<u>SORNS Number</u>	<u>SORNS Name</u>
Treasury/IRS 22.061	Information Returns Master File (IRMF)
Treasury/IRS 24.046	Customer Account Data Engine Business Master File
Treasury/IRS 34.037	IRS Audit Trail and Security Records System

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
Integrated Production Model (IPM)	Yes	10/27/2017	Yes	04/01/2015

11b. Does the system receive SBU/PII from other federal agency or agencies? No

11c. Does the system receive SBU/PII from State or local agencies? No

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

12a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
Business Master File (BMF)	Yes	03/08/2018	Yes	01/29/2018

Identify the authority and for what purpose? 26 USC 6109 is the authority for SSNs in IRS systems. 26 USC 6109 requires inclusion of identifying numbers in returns, statements, or other documents for securing proper identification of persons required to make such returns, statements, or documents. The name, Taxpayer Identification Number (TIN), and address are required to identify the taxpayer's account. The income, deductions, credits, etc. reported on the tax return, as well as any payments received, are required to settle the taxpayer's account, and maintain a record of taxes assessed, abated and collected.

12b. Does this system disseminate SBU/PII to other Federal agencies? No

12c. Does this system disseminate SBU/PII to State and local agencies? No

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12e. Does this system disseminate SBU/PII to other Sources? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?

The system uses data entered from tax returns filed by taxpayers. They are notified of such collection by the Privacy Act Notice in the tax return instructions. Notice, consent and due process are provided via IRS systems and the tax returns filed by taxpayers, pursuant to 5 USC.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? Tax returns filed by taxpayers are the source of data input into the system. Notice, consent and due process are provided via IRS systems and the tax returns filed by taxpayers, pursuant to 5 USC.

19. How does the system or business process ensure due process regarding information access, correction and redress?

The Taxpayer Bill of Rights publication 1 at <http://core.publish.no.irs.gov/pubs/pdf/p1--2014-12-00.pdf> outlines the baseline for 'due process' that business follows. Notice, consent and due process are provided via IRS systems and the tax returns filed by taxpayers, pursuant to 5 USC.

I. INFORMATION PROTECTION

20. Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated). IRS Owned and Operated

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

<u>IRS Employees?</u>	<u>Yes/No</u>	<u>Access Level (Read Only/Read Write/ Administrator)</u>
Users	Yes	Read-Only
Managers	Yes	Read and Write
Sys. Administrators	Yes	Read and Write
Developers	Yes	Read and Write

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Management will determine the access to data by users based on a need to know. However, user access is required to be granted access through the Online 5081 (OL5081) process and the user's manager must sign for the user's access. Role based access is in place that has to be approved by management.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act? Yes

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? No

22b. If **no**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

BMF CCNIP is unscheduled. A request for records disposition authority for BMF CCNIP and associated records will be 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 system inputs, system data, outputs and system documentation will be published in Records Control Schedule (RCS) Document 12990, exact RCS chapter and item number to be determined.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 8/24/2017

23.1 Describe in detail the system s audit trail. Audit Trail Information (including employee log-in info): Type of event; Source of event; Time of event; Date of event; User accountable for event. BMF CCNIP has an ESAT approved Audit plan however it has not been implemented by Enterprise Security Audit Trails (ESAT) at this time. BMF CCNIP is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: In Process

If **in process**, when is the test plan scheduled for completion? 7/31/2018

24.3 If **completed/ or in process**, describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

1. Appropriate privacy-related reviews and assessments are conducted on a yearly basis. 2. Reports on the effectiveness of privacy controls are regularly generated and reviewed. 3. As changes in operations or authorizations occur, requirements for PII collected or otherwise used are revalidated. 4. Auditing Controls were implemented to automatically and appropriately limit PII that is input, produced, transferred, stored, or viewable and to properly destroy it when no longer required. 5. BMFCCNIP is designed such that access to PII is granted only to authorized users with a business need for the information. And this authorization is reviewed monthly. 6. Every action or process that involves the use of PII is attributable to a specific authorized individual, process, or system via our Audit log and NTIN process. 7. BMFCCNIP is capable of appropriately supporting access, correction, and redress.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? Yes

25a. If **yes**, was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request? Yes

If **yes**, provide the date the permission was granted. 10/26/2017

25b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments? Yes

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

26a. IRS Employees: Not Applicable
26b. Contractors: Not Applicable
26c. Members of the Public: More than 1,000,000
26d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804*? No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent? No

End of Report
