

NOTE: The following reflects the information entered in the PIAMS website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: February 25, 2014

PIA ID Number: **748**

1. What type of system is this? Non-Major System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Joint Operations Center National Data Center, JOC NDC

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

Number of Employees: Under 50,000

Number of Contractors: Under 5,000

Members of the Public: Not Applicable

4. Responsible Parties:

NA

5. General Business Purpose of System

The JOC NDC is a minor application that is used to assist the IRS and its partner states with detecting and tracking trend activities that have an ultimate bearing on the collection of fuel excise taxes. The JOC NDC is used for the enforcement efforts of the Safe Accountable Flexible Efficient Transportation Equity Act: A Legacy for Users of 2005 (SAFETEA-LU) legislative requirements to develop, operate and maintain databases to support tax compliance efforts. It is intended to provide a centralized automated solution to analyze patterns of non-compliance, which tend to evolve over time, as offenders identify new schemes to evade excise taxes. The JOC NDC enables state and federal motor fuel tax compliance activities, fosters interagency and multi-national cooperation, and provides strategic analyses of domestic and foreign motor fuel distribution trends and patterns. The JOC NDC works toward those ends through the innovative use of technology and other means, to collect, analyze and share information, and conduct joint compliance initiatives. The JOC NDC is a business activity of the IRS Excise Tax program in partnership with certain member states that have executed a Memorandum of Understanding with the IRS. The JOC NDC includes the organization, business processes and staff that work and support the collaborative environment. The JOC NDC includes the Information Technology (IT) assets of the private network, and specifically does not include the IRS network or associated devices that are not connected to the JOC NDC's private network. Due process is provided pursuant to 26 USC

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact *Privacy and request a search) Yes

6a. If **Yes**, please indicate the date the latest PIA was approved: 04/20/2011

6b. If **Yes**, please indicate which of the following changes occurred to require this update.

• System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No

• System is undergoing Security Assessment and Authorization Yes

6c. State any changes that have occurred to the system since the last PIA

Undergoing eCM-r

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes
9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems	<u>Yes</u>	
Employees/Personnel/HR Systems	<u>Yes</u>	
Other	<u>No</u>	<u>Other Source:</u>

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	No	No
Social Security Number (SSN)	No	No	No
Tax Payer ID Number (TIN)	Yes	No	Yes
Address	Yes	No	No
Date of Birth	No	No	No

Additional Types of PII: Yes

PII Name On Public? On Employee?

FEIN	Yes	No
SEID	No	Yes
Badge	No	Yes
POD	No	Yes

10a. What is the business purpose for collecting and using the SSN ?

If you answered **Yes** to Social Security Number (SSN) in question 10, answer **10b**, **10c**, and **10d**.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

Describe the PII available in the system referred to in question 10 above.

Most of the data comprising PII that arrives into the JOC NDC is via the Excise Files Information Retrieval System (ExFIRS) system Name: for Names of Taxpayer, JOC NDC end-users and JOC NDC system administrators TIN/FEIN: for Taxpayers and JOC NDC end-users Standard Employee Identifier (SEID), Badge Number, Position of Duty (POD) information: for JOC NDC end-users and JOC NDC system administrators

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

Audit information captured on system activity is in compliance with Internal Revenue Manual (IRM) 10.8.3 Auditing Security Standards. Information captured includes: - When an event occurred and results - User initiating the event - Type of event – logon/off; all system administrator and database administrator actions

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If **Yes**, the system(s) are listed below:

System Name **Current PIA?** **PIA Approval Date** **SA & A?** **Authorization Date**

ExFirs Yes 03/01/2011 Yes 06/20/2011

CDW Yes 12/14/2012 Yes 01/24/2012

b. Other federal agency or agencies: Yes

If **Yes**, please list the agency (or agencies) below:

United States Coast Guard (USCG) Cargo reports Vessel movement data Customs and Border Protection (CBP) Facilities information at US ports Port information United States Army Corp. Of Engineers (USACE) Latest USACE docks Cargo moves Department of Transportation (DOT) Vehicle identification numbers Department of Energy (DOE) Codesets used by EIA List of facilities within specified areas Company level imports Environmental Protection Agency (EPA) EPA FRS Facilities Federal Tax Administrator (FTA) Product Codes

c. State and local agency or agencies: Yes

If **Yes**, please list the agency (or agencies) below:

Arizona Supplier Filings State audit and compliance history and results California Terminal disbursements Ending inventory Product codes List of taxpayers listed as farmers Taxpayer and account information Terminal receipts North Carolina Terminal disbursements Ending inventory Product codes List of taxpayers listed as farmers Taxpayer and account information Terminal receipts Texas Terminal disbursements Ending inventory

Product codes List of taxpayers listed as farmers Taxpayer and account information Terminal receipts Virginia terminal, transporter and supplier filings

d. Third party sources: Yes

If yes, the third party sources that were used are:

Publicly available information from the Internet Product codes used by the IRS and states Privately purchased for subscription from companies (e.g. IHS–Fairplay) Pipeline information Ship registries Ship movements Vessel type coding

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: No If **Yes**, specify:

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

The data is required for the administration of the IRS Excise Tax program as a whole. All use of data is relevant and necessary to the successful completion of Excise Tax program objectives, including the detecting and tracking trend activities that have an ultimate bearing on the collection of fuel excise taxes. The JOC NDC is used for the enforcement efforts of the Safe Accountable Flexible Efficient Transportation Equity Act: A Legacy for Users of 2005 (SAFETEA-LU) legislative mandate to develop, operate, and maintain databases to support tax compliance efforts.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct tax administration	<u>Yes</u>
To provide taxpayer services	<u>No</u>
To collect demographic data	<u>No</u>
For employee purposes	<u>No</u>

Other: No

If other, what is the use?

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) Yes

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)	No		
State and local agency (-ies)	Yes	NY, NC, VA, TX, AZ, CA	Yes
Third party sources	No		
Other:	No		

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	_____	_____
Web Beacons	_____	_____
Session Cookies	_____	_____

If other, specify:

Other: _____

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? No

18a. If **Yes**, how is their permission granted?

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? No

19a. If **Yes**, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If **Yes**, please provide the corresponding form(s) number and name of the form.

3140	11C	Filings for occupational Tax and Registration Return for Wagering
3141	2290	Heavy Highway Vehicle Use Tax Returns
3142	720	Excise Tax Returns
3143	8849	Excise Tax credits
3144	637	Excise Tax Registrant
3145	5741	Information Return of U.S. Persons With Respect to Certain Foreign Corporations

20b. If **No**, how was consent granted?

Written consent

Website Opt In or Out option

Published System of Records Notice in the Federal Register

Other:

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Contractor Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	<u>Yes</u>	
Users		<u>Read Only</u>
Managers		<u>No Access</u>
System Administrators		<u>Read Write</u>
Developers		<u>No Access</u>
Contractors:	<u>Yes</u>	
Contractor Users		<u>Read Only</u>
Contractor System Administrators		<u>Read Write</u>
Contractor Developers		<u>No Access</u>
Other:	<u>No</u>	

If you answered yes to contractors, please answer **22a.** (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation? Yes

23. How is access to the PII determined and by whom?

All JOC NDC users must first complete the On-Line 5081 (OL5081) to obtain an IRS SEID. The users may be granted an IRS laptop, where they can check their email and have access to the IRS Intranet for use in their daily jobs such as access to Human Resource policies, bulletins, etc. Once a user has completed the OL5081, they will be granted the SEID, which will be the same identification (ID) used in the JOC NDC. There is no connection between the IRS network and the JOC NDC, but the SA will be made aware of the SEID and use the same one for the user on the JOC NDC. The JOC NDC has only six organizational users and all of them have read-only access.

The six read-only access users will be approved by the administrators, as well as the JOC NDC ISSO. The JOC NDC has only four users that are non-organizational users and they are the administrator users of the JOC NDC. All non-organizational users must utilize both a user ID and a password to gain access to the JOC NDC. The non-organizational users' access will be determined by the JOC NDC ISSO.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

Although there are many sources where the data comes from, the data is manually loaded into the JOC NDC. There are two checks for the data: - Completeness – ensuring that the record counts from the load equaled the total record counts in the JOC NDC. - Accuracy – ensuring that the control totals from the load equaled the totals put into the JOC NDC.

25. 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? Yes

25a. If **Yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

An Excise request for records disposition authority that encompasses JOC, ExFIRS and other Excise data 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 JOC-NDC recordkeeping data and associated records will be published in Document 12990 under Records Control Schedule (RCS) 23 for Tax Administration - Examination, item number to be determined. Several different dispositions have already been approved for the destruction/deletion of ExFIRS application data under Job No. N1-58-12-8. Notice of these disposition instructions is published under RCS 23, item 84. CDW data is approved for destruction 10 years after end of the Processing Year or when no longer needed for operational purposes, which-ever is later (Job No. N1-58-10-7). When next updated, CDW disposition instructions will be published as item 54 under RCS 27 for Compliance Research.

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.

An Excise request for records disposition authority that encompasses JOC, ExFIRS and other Excise data 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 Excise-related recordkeeping data and associated records will be published under IRM 1.15.23 Records Control Schedule for Tax Administration – Examination, item number(s) to be determined.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

To gain access to the JOC NDC, one must be approved and authorized. They must undergo an IRS background check. These users may have been issued an IRS laptop. If a user with an IRS issued laptop visits the JOC NDC, they may need to view JOC NDC data on their IRS issued laptop. In order to do so, the JOC NDC manager and ISSO must first approve the transfer of read-only data. The JOC NDC network remains a private network segregated from all other networks, including the Internet by firewalls and other controls. This is accomplished by the addition of a demilitarized zone (DMZ) between the IRS Enterprise Network and the JOC NDC. The JOC NDC DMZ is a dual-firewall design with front-end and back-end DMZ firewalls supplied by different manufacturers. All data within the JOC NDC is read-only. Data is loaded into JOC NDC databases as received from these respective sources, without edits or updates performed on the data. The data is only verified and validated by the JOC Lab prior to entry into the JOC NDC. Users can query data (via Clementine – Tools described below) in support of their respective business and job functions within the JOC NDC, but user input and update of this data are prohibited through controls implemented at the system level.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

All portable computers connected to the JOC NDC also have WinMagic Disk Encryption software installed. This application encrypts the entire hard disk. The portable devices are secured to the desk utilizing a cable lock and are not to be removed from the JOC NDC. All backups are written to Linear Tape Open (LTO) tapes utilizing the NetBackup application. Encryption is applied for all backup policies. Most of the data comprising PII that arrives into the JOC NDC is via the Excise Files Information Retrieval System (ExFIRS) system, which is part of the IRS. ExFIRS sends this data as a flat-file transfer to the IRS Tumble Weed Server, which is located at the Enterprise

Computing Center-Martinsburg (ECC-MTB) so that it can be made available to the JOC NDC. The SDT project utilizes a FIPS 140-2 validated file transfer product, and transfers files over the Internet using the SSL/HTTPS protocol. All data is transported manually via sneaker-net and uses the IRS-approved Symantec Endpoint Encryption (SEE) software which utilizes AES 256-bit encryption. Prior to data being transported to the JOC NDC, it is verified and validated at the JOC Lab. The data is contained on a CD or DVD while in transport. All SBU digital and paper media is protected during transport using locking Pelican cases. The Pelican cases are fire-proof, steel cases with a combination lock. They are specifically made for the transporting files or other related goods.

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

The JOC application completes monthly IRS mandated Windows Policy Checker (WPC) and Security Content Automation Protocol (SCAP) compliance checker scans required for security and SA&A for all JOC systems, both private and virtualized. Scans (pre-tests) are also run on any new systems, private and virtualized, prior to and immediately after joining the JOC NDC domain. In addition, the system employs Symantec Endpoint Protection for proactive monitoring of JOC application systems. The Symantec Endpoint Protection Center performs a complete virus scans of all servers and workstations on the network on a weekly basis. The scans are regularly scheduled to run on a monthly basis. These scans are analyzed and generally no weaknesses are identified, however, if there are weaknesses noted from the Windows Policy Checkers or SCAP Scans, the JOC application management will share this information with IRS personnel in terms of assessing overall risk at the enterprise level. Any weaknesses noted will be posted on a SharePoint site on the IRS network from via one of the IRS issued computers that are not connected to the JOC NDC. Any weaknesses will also be shared with the SBSE SPMO on a monthly basis. Weaknesses and issues identified are resolved at the time that they are identified, and scans are then re-executed before submission. In the case where a solution is not readily identifiable or resolution is more involved, a risk mitigation plan will be submitted to the SBSE PMO identifying the weakness or issue, the risk identified, and a plan on how to mitigate or contain the risk until a solution can be implemented. The JOC security team conducts a self-assessment on the JOC application on an annual basis. The application will be tested to meet FISMA requirements, evaluating its management, operational, and technical controls in accordance with NIST SP 800-26. Furthermore, each week the JOC security specialist reviews audit logs for any access and password activity compliances.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate*)? No

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If **YES**, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

22.060	Automated Non Master File
24.046	Customer Account Data Engine Business Master Fi
34.037	Audit Trail and Security Records System
42.002	Excise Compliance Programs
42.008	Audit Information Management System

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

32a. If **Yes** to any of the above, please describe:

NA