Date of Approval: April 27, 2017 PIA ID Number: **2502**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Integrated Financial System, IFS

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.

Integrated Financial System, IFS, 838, O&M

Next, enter the **date** of the most recent PIA. 9/2/2014

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

Yes	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
No	Significant Merging with Another System
Yes	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? Yes

If yes, explain what changes were made. A new module is being added to the IFS system via the commercial-of-the-shelf (COTS) Systems Applications and Products (SAP) Supplier Relationship Management product. The new Procurement for Public Sector (PPS) module will add purchasing and contract management functionality to IFS that was previously performed by the Integrated Procurement System (IPS). Once this module is deployed, the IPS application will be retired.

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
Yes	Preliminary Design/Milestone 3
Yes	Detailed Design/Milestone 4A
No	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	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.

IFS is an integrated COTS enterprise resource planning (ERP) software package developed by SAP and is certified by the Financial Systems Integration Office (FSIO) as complying with all federal laws and generally accepted accounting standards. IFS is a standard ledger system that provides FSIO-compliant financial data management and reporting for IRS administrative accounting. The principal user organizations of IFS are the Chief Financial Officer and Procurement . IFS enables the IRS to integrate the majority of its financial processes, share common data across the entire organization, and produce and access information in a real-time environment. IFS provides core financial capabilities, including: general ledger management, core financial management, funds management, budget execution, budget formulation, accounts payable (including W2/1099 tax reporting), accounts receivable, cost management, financial reporting, cash reconciliation, human resources (HR), and travel . In addition, IFS' PPS module provides purchasing and contract management capability. Due process is provided pursuant to applicable federal statute pertaining to financial records, procurement and the Federal Acquisition Regulations.

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 No On Spouse No On Dependent

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

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

The PII data is reviewed regularly and analyzed to ensure the information that is processed by IFS is necessary for daily operations. Payroll and personnel reports have been modified to create a non-SSN version to meet user requirements. This non-SSN version contains only the last four digits of the SSN for an individual and the name of the individual. There is an informal process in place to transition users of the SSN roles to the non-SSN roles. There are no transactions processed within the systems. Distinct roles must be designated for each IFS user.

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.

Selected	PII Element	On Primary	On Spouse	On Dependent
No	Name	No	No	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	No	No
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
Yes	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
No	Tax Account Information	No	No	No

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

Selected	SBU Name	SBU Description
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
Yes	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? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system. Employee purchase card numbers.

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

No	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	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 information system is processing PII for the following purposes: 1. to support external financial reporting to the Office of Management and Budget and Treasury; 2. to support ad-hoc Congressional inquiries; 3. to support the IRS administrative financial management functions (general ledger, budget formulation, payroll, vendor payments, and budget reconciliation, etc.) and 4; to support IRS acquisitioning and contract management. Vendor Taxpayer Identification Number/SSN – Used to group vendors and support issuance of 1099.

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

Auditing of user access to IRS applications, systems, buildings, and networks are logged in accordance with IRS Internal Revenue Manual (IRM) 10.8.1.4.2 Physical and Environmental Protection, IRM 10.8.1.5 Technical Controls, and IRM 10.8.1.5.3 Audit and Accountability. Each data element of PII is verified for accuracy, timeliness, and completeness. All external data feeds into IFS are bound by business agreements that specifically define processing rules from the authoritative source. The accuracy of that information provided to the IRS is guaranteed by the supplying party to contain only relevant, requested, timely, and accurate data. IFS has a system of error handling, trigger files, and manually review processes to ensure that data received by the system is accurate for the processing requirements defined by the applicable interface or internal COTS module. The data used is obtained from the IRS authoritative sources (i.e. Treasury, Accenture, and General Services Administration) as per delivery schedule and by signed agreement. These sources are bound by business agreements that mandate that they only send accurate, relevant, and timely data that is used to support their respective processing into IFS. File transfer methodologies use two techniques to verify file transfers as being complete: 1. Use of a trigger file to indicate start of a transfer condition; and 2. No trigger file. By using a trigger file, the process checks for an existing trigger file. If one exists on the target server, it aborts the process. This indicates that the file has not been picked up or has been processed by the target system. After the successful completion, a trigger file is then created as an indication that a file transfer

process has been completed. In both cases, the file transfer makes redundant connections for verification making sure the waiting process is not triggered by the arrival of a file in the data file transfer area. Any file transmission and communications error received during transfer is written to an audit log and a broadcast message is sent to a pre-defined mailing list of operating personnel (tier-level support). If a data transfer error occurs, therefore showing incompleteness, the data is either rejected or sent back to the source system for correction. Manual intervention by authorized IFS users is required to correct data value to allow IFS processing. In order to maintain current data, files are transferred as defined by the Tivoli scheduler process component of the IFS solution. The Informatica component used by the IFS has a built-in logic to prevent processing of duplicate files. IFS transfers files based on the defined business requirement either on a daily, weekly, monthly, yearly, or as needed basis. For external IFS connections, those systems, by signed agreement, are considered authoritative sources by the IRS and the data received from them is understood to be current, accurate, complete and relevant by established business rules and signed IRS connection agreements. IFS data transfer that ensure data currency are as follows: Disbursements; Payments; Validation Files; US Treasury Accounting string validations to procurement, travel, and payroll interfaces; Mass Print (DCC Print); Detroit data center mass printing; Treasury User Fees (Pay.Gov); User fees; AINFC Automated Interface from National Finance Center; Treasury User Fees (eServices); GLASS (GWA); Cash Reconciliation; W2 Information for SSA and States; SAAS Security and Audit System Logs; 1099 Information; GovTrip (Credit Card Services) Travel Reimbursements; WebTRAS Travel Reimbursements; GRAS Relocation Reimbursements; OL5081 Travel Registration. Prior to release to the production environment, extensive testing is performed to verify the accuracy, timeliness and completeness of the data elements. Format masks, edit checks, and referential integrity checks are also used to ensure accuracy and completeness

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.

SORNS Number	SORNS Name
Treasury/IRS 34.047	IRS Audit Trail & Security Records
Treasury .009	Treasury Financial Management System
Treasury/IRS 22.012	Health Coverage Tax Credit Program Records

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.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Government Relocation Accounting System Travel Reimbursement Accounting System) (GRAS (TRAS))	Yes	03/19/2016	No	
Automated Interface with the National Finance Center (AINFC)	No		No	
General Ledger Account Support System (GLASS)	No		No	

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

If **yes**, for each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA)/Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Movelinq	SFTP	Yes
Treasury (Pay.gov)	https	Yes
GSA (Concur)	SFTP	Yes

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
AINFC	SFTP	No
GRAS	SFTP	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.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
IMF	Yes	03/16/2017	Yes	11/14/2016

Identify the authority and for what purpose? The IFS Change Control Board (CCB) approves the dissemination of all SBU/PII being distributed to external systems.

12b . Does this system disseminate SBU/PII to other Federal agencies? Yes

If **yes** identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU)

Organization Name	Transmission method	ISA/MOU
Concur	SFTP	Yes

Identify the authority and for what purpose? The IFS CCB approves the dissemination of all SBU/PII being distributed to all systems.

12c. Does this system disseminate SBU/PII to State and local agencies? Yes

If **yes**, identify the full names of the state and local agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Various	SFTP	No

Identify the authority and for what purpose? The IFS CCB approves the dissemination of all SBU/PII being distributed to all systems. Individual state tax agencies receiving data from IFS changes yearly based on IRS employee travelers state of residence. Many states require employers to file W2s for employees receiving travel-related one day taxable subsistence. Additionally some state tax authorities require W2s for employees receiving relocation reimbursements from the IRS.

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, cloud, 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? No

17b. If **no**, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.
The information within IFS is employee and vendor PII which comes from various IRS Systems. Those systems provide the Privacy Act Notice to individuals. IFS does not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent and due process are provided in the tax forms instructions, and 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? The information within IFS is employee and vendor PII which comes from various IRS Systems. Those systems provide the Privacy Act Notice to individuals. IFS does not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Due process is provided pursuant to applicable federal statute pertaining to financial records, procurement and the Federal Acquisition Regulations. Due process is provided 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

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

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? No user access is allowed until an IRS Online 5081 (OL5081) application is completed by the requestor and approved by the IRS. The IFS SAP user configurations and privileges are based on defined role-based profiles and are granted through the OL5081 process. Access is further controlled in a Windows environment with a user profile assigned with user-specific data that restricts the user's

working environment. This record can include display settings, application settings, file privileges, and network connections to be accessed.

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? Yes

22a. 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.

All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6. Records are scheduled under the General Records Schedules, IRS Document 12829. 1.1 for Financial Management and Reporting Records, Item 010; and Records Control Schedule 16 for Finance-Chief Financial Officer and Accountable Officer Records (published in Document 12990). Financial records data must be retained for at least 6 years, 3 months after the funds have expired/after period covered by account. If the PII data related to a less stringent retention policy were purged, then that data element would not be available for future processing on a connection that requires a longer retention period, i.e. payroll, W2/1099.

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)? In-process

23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion? 9/26/2017

23.1 Describe in detail the system s audit trail. Password Change, including User ID and Terminal ID; File Create including file name; File Delete including file name; File Open including file name; File Close including file name; Program initiation; Time and date stamps for key transactions; Date and time that the event occurred; The unique identifier (e.g., user name, SEID, application name, etc) of the user or application initiating the event; Type of event; Subject of the event (e.g., the user, file, or other resource affected) and the action taken on that subject; The outcome status (success or failure) of the event.

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? 5/22/2017

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?
User roles testing has occurred to ensure that user roles provide only the approved access. The IFS Audit Plan and Interconnection Control Document has been updated to include new PII elements. Auditing capability will be tested early May 2017. A SBU Data Use Questionnaire has been submitted to Privacy who confirmed that a SBU Data Use Request is not required for this system. Prior to deployment, the system will undergo System Integration and System Acceptance testing to ensure separation of duties and role based access control. The system will also undergo a Cybersecurity Security Control Assessment to validate that all required security controls are in place.

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. 3/14/2017

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: Under 50,000
26b. Contractors: Under 5,000
26c. Members of the Public: Not Applicable
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