Integrated Financial System (IFS) – Privacy Impact Assessment

PIA Approval Date – June 3, 2008

System Overview

IFS data is transmitted to other internal IRS applications, other Federal agencies, and data that is collected from IRS employees or business partners, i.e. healthcare providers. It describes how the accuracy, completeness, and prevalence of the data is ensured.

Data in the System

1. Generally describe the information to be used in the system in each of the following categories:

In general, IFS does not process taxpayer information, all processing in associated with employee benefits, payroll, travel, medical, government inter-agency processing, or IRS facility space allocations. The IFS system includes core financial management, general ledger, budget formulation, accounts payable, accounts receivable, funds management, cost management, and financial reporting.

- Personal information of the IRS employees - The following information is collected by IFS as needed to process monetary transactions with members of public to pay invoices and other reimbursements:
  - Name (First name, Last name, Middle name)
  - Home Address (of record)
  - Telephone Number (Business)
  - E-mail Address (IRS)
  - Bank Routing Information (Account for Deposit)
  - Taxpayer Identification Number (TIN) / Social Security Number (SSN)
  - Invoicing and billing processing information

Note: *For specific information in relationship to Personally Identifiable Information (PII) data elements process by Northrop Grumman GovTrip interfaces, please refer to the referenced PIA documents identified by this document.*

Aggregated data for seized assets is maintained in accordance with Integrated Financial (IFS) System Trusted Facility Guide Document No. <PRIME-IFS-DOC-TrustedFacilGuide.doc> version2.0 dated October 31, 2005. IRS employee W-2 information is processed to reflect employee taxable travel expenses incurred.

Note: *It should be noted, that for this entire document and for processes identified as relevant to IFS application that all identified IRS PII data elements exist within the IFS Oracle database. The data retained by external entities are not controlled by the IFS application, but rather is secured and protected in accordance with IRS business agreements signed by both responsible parties. Data that resides outside of the IRS is the sole responsibility of that party, specifically the Social Security Administration, U.S. Census Bureau, U.S. Department of the Treasury, Financial Management Services, U.S. General Services Administration, and Northrop Grumman.*

- Employee - The following employee information is collected to process payroll and monetary transactions with employees such as travel and medical reimbursements. The IFS application contains the following PII employee information to allow for the proper financial accounting of monies disbursed to employees:
  - Name
    - (Last name, First name, Middle name)
  - Social Security Number (SSN)
    - For W-2 tax form submittal
    - For 1099 tax form submittal
  - Employee ID
    - (IRS SEID)
  - Home Address
    - Street, Apt. No., City, State, Zip Code
  - Bank information
    - Bank Routing Number
    - Bank Account Number
  - IRS E-mail Address
  - Gender
  - Veteran and Educational Statuses - Required to support the U.S. Census Bureau demographic studies. No associated PII data is transferred with this benign Veteran or Educational data.

Note: *For specific information in relationship to PII data elements process by Northrop Grumman GovTrip interfaces, please refer to the referenced PIA documents identified by this document.*

Other – All other information collected or distributed to IFS is for used for accounting and financial processing as designed by the COTS functional capabilities of the system and does not specifically identify any person or organization specifically. The Treasury FMS Pay.gov connections does not use taxpayer data or employee data but rather uses generally accepted accounting data for reconciliation of third party billing and payments for electronic distribution of transcripts. Other data includes:

- Budget execution data
- Receipt and receivable data
- Cost management data
- Procurement data and vendor information
- General Ledger data

Note: *For specific information in relationship to PII data elements process by Northrop Grumman GovTrip interfaces, please refer to the referenced PIA documents identified by this document.*

2. What are the sources of the information in the system?
The Integrated Financial System (IFS) interfaces with nine external and eleven internal applications systems to obtain its financial information.

The PII related data for these interfaces are

- AINFC
- EPIP
- eServices
- GDI
- Govtrip
- GRAS
- HCTC
- HR_CONNECT
- IFS (SAAS)
- IFS Disbursement
- IFS PRINT (AR/Invoices)
- IFS PRINT (W2_info)
- IFS PRINT(1099_info)
- IFS(Govtrip)
- IFS(Validation)
- IFS(WebTRAS)
- PayGov
- SETR
- Source
- TIER
- WebIPSRTS
- WebTRAS

Note: *All PII data within IFS, regardless of the associated connection, is retained for a minimum of 7 years 1 months. Due to the structure of the relational database, PII data elements are a shared information repository and not a distributed or replicated model. 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.*

In addition, sensitive data, such as the identified IRS PII data elements are obtained through the same means of secure communication (i.e. VPN technology, SecureFTP, digital certificate exchanges) and are used for the sole purpose of IRS wide payroll reconciliation activities. These interfaces use batch-file transfer technology that is machine based in its authentication and authorization mechanism. This eliminates man-in-the-middle attacks by removing the human component intervention needed for routine processing. Only when errors or trigger files demand that reprocessing occur does an authorized IRS employee manually intervene to invoke the new processing routine.

Social Security Administration (SSA)

The SSA file is extracted from IFS and transmitted to Social Security Administration using Connect Direct, through an IRS mainframe environment located in DCC. The SSA file is transmitted on an annual basis. The selected batch job scheduler triggers the batch program to process these files, which validates the file existence and IFS system support is notified for any SSA process failures. The original files are saved in the archive directory by calendar year.

Health Coverage Tax Credit (HCTC) - Accenture

The IRS is responsible for administering the HCTC program in which eligible employees or pensioners with qualified health coverage pay 35 percent of their health plan premium each month with the IRS paying the remaining 65 percent to provide full coverage to the individually designated health care providers. The monthly files are delivered through a drop-box located in the De-Militarized Zone (DMZ) segment at DCC using a secured VPN tunnel. There are no PII data elements transferred via the HCTC interface. The system of record notice for the HCTC data elements is Treasury/IRS 22.012-Health Coverage Tax Credit Program Records

U.S Treasury (Disbursements, WebTier, HRConnect)

On a daily basis, IFS creates payment data records for all payments approved and made ready for processing. These payments are to external vendors and IRS employees (internal vendors). Payment data records are classified under four categories:

1. Electronic File Transfer (EFT) payments to vendors in CCD+ (Cash Concentration Disbursement Plus) format. Addenda records attached to these payment records provide invoice and interest payment information for the Payment Advice Internet Delivery (PAID) system
2. EFT payments to employees in PPD+ (Pre-Arranged Payment and Deposit Plus) format
3. Checks to vendors and employees
4. Pre-notification (pre-note) data (prior to initiating EFT) for vendors and employees

All of the above, except pre-note data, are initiated manually on a daily basis. The pre-note data is scheduled as a nightly batch job when there have been changes to or additions of bank data in the Vendor file. The IFS application creates these payment data files through scheduled jobs and transmits the files to FMS for disbursement.

User Fees (Pay.Gov and eServices)

Pay.Gov is a secure Government-wide financial management transaction portal managed by the U.S. Department of Treasury’s Financial Management Service. It offers a suite of online electronic financial services that Federal agencies can use to meet their responsibilities towards the public. IFS interfaces with Pay.Gov to receive, interpret, and process payment information using https. IFS interfaces with the eServices Transcript Delivery System (TDS), to provide Customer Number and monthly billing information for each mortgage consolidators. The eServices interface is accomplished using direct system connection, Application Program Interfaces (API) to eliminate intermediate files and processes. These APIs exchange data in real-time.

U.S. General Services Administation (GSA)
E-Gov Travel system (GovTrip)

GovTrip is a bi-directional interface between Northrop Grumman and the IRS for exchanging travel disbursement and reimbursement financial data in regards to employee or sponsored IRS traveler transactions. More specifically, in 2008 the interface will support the transfer of data between the Northrop Grumman E-Gov Travel system (eTes), known as GovTrip (www.govtrip.com), and IFS. In support of these objectives, Northrop Grumman and IRS facilitate the exchange of financial information relating to the payment of travel funds for IRS employees. Northrop Grumman and IRS jointly design, develop, and test the mechanisms, methods, and procedures to carry out the transfer and exchange of the following types of data:

- Obligation, advance, and voucher transactions, including transactions pertaining to obligation amendments and supplemental vouchers (sent from GovTrip to IFS)
- E-mail notifications (sent from GovTrip to designated points of contact)
- Advice of payment (AOP) transactions (sent from IFS to GovTrip for successfully processed voucher and advance payment transactions)
- Line of accounting validation and IFS vendor transactions (sent from IFS to GovTrip)

The data exchange between the GovTrip system and a designated IRS “dropbox” server is accomplished using secured Virtual Private Network (VPN) channel that supports file transfer protocol (FTP) transfers and resides within the de-militarized zone (DMZ) of the IRS network. In particular, each file inbound to IFS from GovTrip is transmitted to the “dropbox” server and posted to the to the IRS directory. Any files on the “dropbox” server from the IRS directory are retrieved and downloaded to the GovTrip Enterprise Application Integration (EAI) server. IRS is responsible for transferring data as required between the dropbox server and IFS to support end-to-end requirements. E-mail notifications are sent by the EAI system to designated Northrop Grumman and/or IRS points of contact to provide alert notifications in the event of automated translation failures or other interconnection failures detected by GovTrip. These unencrypted e-mails do not contain any sensitive, personal information.

Note: *See the applicable IFS GovTrip PIA for diagrams and further clarification of this connection. For the 2007 GovTrip interface-testing phase, only sanitized data, non-PII data, was used to verify the IFS-NG interfaces. The data file was transmitted through the production drop box to the test environment. This process was approved by the IRS Office of Privacy and Information Protection for the sanitizing of data.*

The IFS Interfaces fall into two general categories:

- **IRS Internal Systems**: Systems that reside with the IRS IT domain and facilities. These can be further divided into IRS Modernized or Current Processing Environment (CPE) categories.
- **IRS External Trading Partners**: Any system that is not an integrated domain component of the IRS IT Enterprise.

In accordance with the “Sensitive Information and Personally Identifiable Information” memorandum signed by Mr. Daniel Galik, Chief, Mission Assurance and Security Services; now known as IRS Cyber Security, dated June 5, 2006, states that all IRS PII data shall be encrypted during transmission, transport, and storage to prevent the unauthorized readability of any files. Currently, the IFS application has critical transmission segments to utilize secure connections deploying FIPS 140-2 compliant encryption technologies for all existing external and internal interfaces.

2a. What IRS files and databases are used?
External or other internal IRS application files or databases are not utilized by IFS for processing. The IFS COTS solution utilizes an Oracle relational database as the central repository for the IFS PII data elements defined in this document. Only data elements from approved definitive sources i.e. Treasury, FMS, GSA, Accenture, authorized by signed IRS interagency agreements, are inputted into IFS for processing of claims, reimbursements, disbursements, and payroll and end of year tax reporting from the following IFS connections.

1. Automated Interface to the National Finance Center (AINFC)
2. General Ledger Accounts Support System (GLASS)
3. U.S. General Services Administration (External)
    a. GovTrip – Northrop Grumman
4. Web Integrated Procurement System Request Tracking System (WebIPSRTS)
5. Web Travel Reimbursement and Accounting System (WebTRAS)
6. Government Relocation and Accounting System (GRAS)
    a. Shared interface with WebTRAS
7. Accenture (External)
    a. Health Coverage Tax Credit (HCTC)
8. U.S. Department of the Treasury
    a. HRConnect
9. Financial Management System (External)
    a. Pay.gov
    b. Government Wide Accounting (GWA)
    c. Disbursements

2b. What Federal Agencies are providing data for use in the system?
Federal systems that currently provide timely and accurate data to the IRS IFS application are as follows:

- Treasury
    - HRConnect
    - Disbursements
    - WebTIER, and
    - Pay.Gov (FMS)
- Department of Agriculture National Finance Center (NFC)
    - Automated Interface to the National Finance Center (AINFC)
- General Services Administration (GSA)
    - GovTrip – Northrop Grumman

Note: *The Department of Treasury Financial Management System (FMS) provides disbursement data directly to Enterprise Computing Center-Martinsburg (ECC-MTB), which is then transmitted internally (IRS domain) from ECC-MTB to the Detroit Computing Center (ECC-Detroit) for processing within the IFS system.*

2c. What State and Local Agencies are providing data for use in the system?
None, IFS accepts no data or PII elements from State or Local Government agencies.

2d. From what other third party sources will data be collected?

- Accenture
    - Health Coverage Tax Credit (HCTC)
- Northrop Grumman
    - GovTrip

2e. What information will be collected from the taxpayer/employee?

Taxpayer: IFS does not collect any data directly from the taxpayer.
Employee: The accurate data required to process IFS accounting include employees in the Accounts Payable (AP) vendor master file. IFS receives employee payroll and medical account data via the Treasury HRConnect system and the external connection Accenture HCTC interfaces respectively. The following PII data elements within IFS that could potentially identify an IRS employees or vendors have been identified as being either stored or retrieved by the system. In accordance with IRS publication *IRM 10.8.1.3.1.1.2 – Personally Identifiable Information*, the PII data elements to be protected by these interfaces include the following sensitive employee information:

- Full Name
- Social Security Number (SSN) / Taxpayer Identification Number (TIN)
- Date of Birth
- Home telephone number
- Biometric data, (i.e. height, weight, eye color fingerprints)

In addition, the IFS application has identified the following sensitive data elements as potential PII related data that could identify an IRS employee or vendor.

- IRS Employee ID
- Home Address of Record
- Healthcare provider (if not aggregated with other PII data elements listed above)
- Banking information (ABA Routing/Account Numbers.)
- Credit Card Number
- IRS corporate E-mail Address
- Veteran and/or Educational Status (Note: *U.S. Census Bureau – this is a requirement of the U.S. Government to supply requested information to this agency.*)

3a. How will the data collected from sources other than IRS records and the taxpayer be verified for accuracy?
All external data feeds into IFS are bound by business agreements that specifically defined 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.

3b. How will data be checked for completeness?
The data used is obtained from the IRS authoritative sources (i.e. Treasury, Accenture, and GSA) as per delivery schedule and by signed agreement. These sources are bound by business agreements that mandate that only send accurate, relevant, and timely data that are used to support their respective processing into IFS. File transfer methodologies used two techniques to verify file transfers as being complete.

1. Use of a “trigger file” to indicate start of a transfer condition
2. No trigger file

By using a trigger file, the process checks for an existing trigger fie. If one exists on the target server, it aborts the process. This indicates 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.
3c. Is the data current? How do you know?

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 schedules to ensure data currency are as follows:

- 1099 Information
- AINFC
- Disbursements
- ePIP
- eServices
- GDI
- GLASS
- GovTrip
- GWA
- HCTC
- HRConnect
- Interface
- Mass Print
- Pay.GOV
- SAAS
- SETR
- TIER
- Validation Files
- W2 Information
- Web RTSIPS
- WebTRAS/GRAS

4. Are the data elements described in detail and documented? If yes, what is the name of the document?
Yes, All IFS PII data elements for the nine external interfaces and eleven internal interfaces are identified in the applicable IRS Interconnection Diagrams (ICDs), or Design Specification Reports (DSR 1 / DSR 2). These sensitive IT security-engineering documents are in an IRS controlled access repository (DocIT) that requires IRS approval, i.e. OL5081 with manager approval, for a particular role and or user ID is allowed access.

Access to the Data

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

The IFS user community consists of three different types of users:

1. **The IFS end-user**, of which there is approximately 600-1000, are granted access to the system by role and IRS Online 5081 approval processes for access to IRS applications. Each user is then assigned a specific set of roles relevant to his/her job description and IFS user role, which limits their access to only those transactions, processes, or views specifically needed to complete their functional job requirements.
2. **System Developers**, of which there are approximately 20-30, have access to the IFS development environments, to modify the business rules, reports, queries, transactions, etc. to ensure that IFS operations are in agreement with currently defined IRS business requirements. Changes to the production IFS system follow the IRS ELC standard build-promote methodology to ensure all changes to the environment have been tested, verified, and approved prior to their introduction.
3. **System Administrators**, of which there are approximately 10-15, have access to the application. System Administrators are not assigned to any IFS roles that process financial transaction and cannot view sensitive data within the system. These types of users access the production IFS system via the COTS application portal known as the "SAP GUI." This is a fat-client COTS application installed on these authorized workstations to allow for the administration of the application. The processing of PII data from these workstations are protected by using SSL technology, and SecureFTP.

These particular users of IFS resources are IRS employees and have undergone the appropriate employment background investigations and Online Form 5081 approval processes prior to obtaining the level of system access required to perform their duties. Specific details of the assigned roles, transactions and table access permissions may be found in the "*Role Transaction Code Content*" report in the "*Profile Generator of SAP*".

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access will be on a least-privilege basis and will be audited to ensure that IRS polices are being observed. Auditing of user access to IRS applications, systems, buildings, and networks are logged in accordance with *IRS 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*. No user access is allowed until an IRS OL5081 application is filled in by the requestor and approved by the IRS. The IFS SAP user configurations and privileges are based on defined role-based profiles. 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.

2a. Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes, not only are IRS life cycle, engineering, development, and Cyber Security guidelines well documented; in addition, IFS has engineering documentation that specifies the file privileges, network controls, role responsibilities, and application procedures for gaining access to the application. Specific details of the assigned roles, transactions and table access permissions can be found in the IFS report known as "*Role Transaction Code Content*" from the COTS "*Profile Generator of SAP*" program.

3. Will users have access to all data on the system or will user's access be restricted? Explain.

Users only have authorized access privileges, and not unfettered access to all IFS data elements. All users have access to only those data relevant to their assigned role. Please note that majority of the IFS end users have only one assigned role. The IFS data is limited via role-based access, profiles, and separation of duties to ensure that only authorized users can access data and perform transactions as required by their specific job description.

The use of the IRS Enterprise User Portal (EUP) and defined SAP user roles, as well as the ability to audit such user access to employee data increases the level of protection and oversight provided in this application. The use of IRS SEIDs instead of employee SSN has been implemented for new interfaces, such as GovTrip. This reduces the exposure and tracking of employee sensitive information. Currently, IRS Enterprise Architecture version 3.0 applications, such as GovTrip (also known as Northrop Grumman's eTes) are utilizing the use of SEIDs in lieu of SSNs for employee transactions. Legacy IFS connections have not been retrofitted with this capability, but have been identified in IFS "get well" planning.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?
IFS utilize the SAP authorization objects that limits access to PII and sensitive information to the record field levels. Each IFS end user role contains an authorization profile that is made of several authorization objects. These authorization objects define the level of access for each user on the table/filed level. For example, it defines who has read only, update/create or no access to the *Activity* field on the *EMPV* table.

In addition, IFS interfaces with the Security Audit and Analysis System (SAAS) system via a batch, file-based manner. SAP audit logs, which contain information about data manipulations and accesses that have been performed, are transferred to SAAS in the ISS-defined file format. The MITS GSS (2, 18 AND 27) environments that host IFS enforce physical access restrictions as per *IRS IRM 10.8.1.4.2*. Logical access is enforced by IFS with Role-based Access Controls (RBAC) and IRS ELC approved methodologies. The IFS application is designed to distribute security administrative functions as well as to prevent role assignments that would violate the separation of duties and least privilege principles.

Continuous monitoring of all users and the reporting and investigation of incidents are deployed to ensure that malicious, mischievous, or unauthorized browsing of employee data is not occurring. The Office of Financial Systems (CFO) maintains an up-to-date list of personnel that have been authorized to access the application and its data files, i.e. configuration, source code, and data elements. In addition, user/administrative activities are documented in the audit logs in accordance with *IRM 10.8.3, Mission Assurance and Security Services Audit Logging Security Standards*.

System Administrators and developers roles are restricted to prevent any changes to the system without prior authorization. Access to "Live Data" used in the system test environments is controlled in accordance with *IRM 2.5.16, Use of Live Data in Testing*. The term "Live Data" implies that production data is utilized on a case-by-case basis to verify new processes or data transfers.
This data is a snapshot copy of the existing production data that is transferred in accordance with IRS practices for transporting data or media via courier. These processes are defined in the Mr. Dan Galik memorandum. There is a process to renew access to "Live Data" in the system test environment annually.

The “Live Data” is maintained on EITE storage area network (SAN) on a test LPAR on the Mainframe in ECC-Martinsburg. The protection afforded these servers in the data-center include enforced physical access restrictions; with Role-based Access Controls (RBAC); use of Intrusion Detection Systems (IDS); and Enterprise monitored audit trails.

The IFS (SAP) Security Audit Log records security-related system events on IFS components, such as R/3, BW, and SEM. The SAP Portal’s Presentation and Repository servers’ events are logged by the primary operating system auditing system. The SAP Security Audit Log is designed to take a detailed look at what occurs in the IFS application. The Security Audit Log keeps a record of the specified activities of all users. The details of the interface, including data elements and the interval at which this data will be transferred are documented can be found in the *IFS Security Audit and Analysis System ICD, Version 2.2*.

The list below provides IFS security audit review procedures:

Procedure:
Ensure users are on appropriate roles.
Monitoring Procedure: Process Online 5081 requests, verify manager’s approval and review role selection. All users are required to recertify annually through the Online 5081 System.
Frequency: Daily

Procedure: Ensure inactive users are denied access to the system.
Monitoring Procedure: Perform online review using transactional query SUIM (User Information System) and disable accounts of users who have not logged onto the system in 45 days.
Frequency: Bi-Weekly

Procedure: Mitigate separation of duty risks.
Monitoring Procedure: Review report for Critical Combinations of Authorizations at Transaction Start. This procedure ensures that collision of two or more parties are not collaborating to compromise the system.
Frequency: Monthly

Procedure: Maintain integrity of security transactions.
Monitoring Procedure: Perform online review for transactional access to security administration using transaction queries: PFCG – Role Maintenance
SUIM – User Information System
SE38 – ABAP Editor
SU01 – User Maintenance
SM01 – Lock Transactions.
Frequency: Quarterly

Procedure: Maintain accuracy and appropriateness of user roles.
Monitoring Procedure: Coordinate and review with role owners all transactions for appropriateness. Update roles (add/delete transactions) if necessary based on findings.
Frequency: Annually

5.a Do other systems share data or have access to data in this system? If yes, explain.
Yes, other IRS systems share the IFS data as relying third parties; however, access to IFS from other applications is controlled through IRS protected dropboxes located in the IRS IT Enterprise DMZ or the IFS Data Transfer Server (DTS) area located in the DCC data center. In order for IFS to exchange data with other modernized IRS applications or Current Processing Environment (CPE) systems, a data transfer service utilizing a pair of clustered servers, known as DTS have been implemented. This service utilizes file transfer technology to transfer preformatted batch files to and from IFS through approved connections. These connections use secure IT techniques, i.e. VPN, IPsec, SSL, OPENssh, Tumbleweed, digital certificates, and SecureFTP, to transfer or receive data from other systems. All data transfers are controlled by the enterprise job scheduler (ESM Scheduling Service). Incoming files are transferred via an NFS mount to Informatica for Extraction, Transformation, and Load (ETL) process and transfer to the SAP server. Outgoing files use the same ETL processing method, and then transferred via an NFS mount to the data transfer server for subsequent transmission to the appropriate system.

The CIM (Connection Information Manager) utility at the operating system level runs in the background to verify passwords and other login credentials. This information is checked against information stored in Oracle table (Encrypted). Data Integrity: Data file level - The process checks for a duplicate file by comparing files from archive. If the file match is found, the process aborts with a warning: duplicate file. Data Field level: The total number of records, header records and trailer records are created for IFS SAP R/3 for verification. The data fields also must pass the integrity checks of the application.

5b. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?
The Office of Financial Systems (CFO) is the guardian to ensure that the IFS application is protecting personally identifiable information. For external connections, the applicable Interconnection Service Agreement (ISA) signed by the identified Designated Acting Authority (DAA) or business owner of each trading partner identifies the custodian of the system and for ensuring that due diligence of practices is adhered to by all users of the system.

6a. Will other agencies share data or have access to data in this system (International, Federal, State, and Local, Other)?
Yes, the IRS and IFS shares data with other federal agencies, and State governments (for tax from submissions) as per agreement. Currently, the agencies approved by the IRS to connection to (for the purpose of supplying or receiving information) IFS are as listed below.

- Treasury
  - TIER
  - HRConnect
- Accenture
  - Health Coverage Tax Credit (Contracted system)
- Social Security Administration
  - W2
  - 1099
- General Services Administration
  - Northrop Grumman GovTrip (Contracted shared service provider)
- U.S. Treasury Financial Management Services (FMS)
  - Disbursements
  - Government Wide Accounting
  - Pay.Gov

6b. How will the data be used by the agency?

The following bulleted items reflect the PII data elements used by the relying party.

- Department of the Treasury:
    - The **Disbursements** system creates and transfers to Treasury a formatted file to facilitate disbursements by Treasury. Disbursements include vendor checks/EFTs and employee checks/EFTs for travel and relocation expense reimbursement, travel advances, non-travel related expenses and emergency salary payments (ESP). Payroll-related disbursements are not included.
        - **TIER** provides IFS financial data to Treasury to facilitate department-level external reporting. The data include information necessary for FACTS I, FACTS II, SF-133, and SF-2108 reporting.
    - **HRConnect** Synchronizes cost centers and related information between the human resources system (HR-Connect) and IFS.
    - **Government Wide Accounting (GWA)** The IFS SAP BW Cash Reconciliation reports and queries based on the Government Wide Accounting and Reporting (GWA) monthly reports extracted in text files. These extracted files are sent to the IFS data transfer server for transformation. The Informatica process transforms and prepares files for loading into SAP BW.
    - **Health Coverage Tax Credit (HCTC):** The HCTC application sends inbound interface file(s) to IFS to create invoices for health care providers and for individual refunds. HCTC is the application the IRS uses to process and manage the following: Invoice creation for health care provider (vendors) and for individual refunds, summary cash position, payment extract advice for clearing.
    - **Social Security Administration:** W2 Information provides employee-level Form W-2 information to the Social Security Administration and each state.
    - **General Services Administration:** Provides IRS employee related data to facilitate the processing of travel logistics. This data contains sensitive and PII related data in regards to employee name, credit card information, bank account information, home of record, contact information, and emergency contact information.

6c. Who is responsible for assuring the proper use of the data?
The Office of Financial Systems (CFO) is responsible for the proper use of all data residing in the application. For external trading partners, the DAA or business owner is responsible for the safe and proper care of all information obtained via their approved connection, as per business agreements.

6d. How will the system ensure that agencies only get the information they are entitled to under IRC §6103?
The handling of IFS vendor account data that includes payroll reconciliation information and employee SSNs is controlled through the Privacy Act requirements. Data being sent to GSA/GovTrip was minimized during discussions that is reflected in the Govtrip PIA and are bound by referenced business agreements that specifically defined processing rules from the authoritative source.

Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?
Yes, as designed and approved by the IRS ELC only PII data elements necessary, as defined in the document, to conduct business as required by the IRS CFO office is obtained on the behalf of the CFO mission by IFS. The data maintained in IFS is relevant and necessary to support the defined IRS functionality specified in its design documents and IRS contractual requirements.
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

Yes, IFS is based on an implementation of SAP, which include data derivation and substitution rules for accounting and financial data that is required to support the IRS business requirements.

2b. Will new data be placed in the individual's record (taxpayer or employee)?
Yes, IFS updates employee records as new information are received from the AINFC and HR Connect interfaces. This is necessary to allow IFS to correctly identify an employee for the timely delivery of payroll, benefits or reimbursements information. The IFS does not maintain any taxpayer data. The IFS is the IRS financial accounting system and does not maintain taxpayer information.

2c. Can the system make determinations about taxpayers or employees that would not be possible without the new data?
Yes, however the IFS system does not make any automated determinations about employees. The new data is necessary to ensure the authorized, safe, and related disbursement or notification is sent to the correct employee or employee's home of record.

2d. How will the new data be verified for relevance and accuracy?
The new data is entered by trusted roles and IRS procedures that require multiple levels of business verification, which ensures that data is relevant and accurate.

3a. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
The IFS implementation includes a SAP Business Warehouse (BW) module that collects information from the AINFC, GLASS, and GWA interfaces and consolidates this data for reconciliation and reporting purposes. The access to the BW module is limited to specific users in the Beckley Finance Center (BFC) that performs payroll and cash reconciliation functionality; and to limited users of the Office of Financial Reporting (OFR) for external reporting requirements to OMB, Treasury and other external agencies.

3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
Yes, to complete monthly and year-end accounting functions; IFS run consolidation processes for these reconciliation activities. The same controls applied to the entire system for data protection and user access, as describe in the document and defined in the applicable ICD/DSR, are enforced for these routines.

4. How will the data be retrieved? Can a personal identifier retrieve it? If yes, explain.
Data within IFS is retrieved by database views within IFS that allow appropriate users to retrieve information based on personally identifiable information data elements. These views are a critical processing component of the IFS system to meet current business requirements. End-users are limited via role-based access (RBAC), profiles, and separation of duties to ensure that users can only access data and perform transactions as required by their specific jobs. In addition, access to the BW module is provided to a limited number of users for payroll/cash reconciliation and external reporting purposes.

What are the potential effects on the Due Process rights of taxpayers and employees of:
4a. Consolidation and linkage of files and systems
IFS is a relational database and the use of files shared by other application components in that manner. IFS has a disaster recovery site in ECC-Memphis where data is replicated every six hours. Extraneous instances of files are not supported by this application, therefore all linkage for IFS interfaces or processes utilize the one controlled instance of that particular data element.

The IFS data replication to the DR site has no effect or restricts the Due Process rights of employees and thus requires no mitigation.

4b. Derivation of data
IFS performs data derivation and substitution, in the R/3 module, that are required to support the IRS financial and accounting functions. The derivation of data performed in IFS has no effect or restricts the Due Process rights of employees and thus requires no mitigation.

4c. Accelerated information processing and decision making
Data is timely and accurate resulting in improved service to the employee and/or taxpayer. The timely and accurate data in IFS has no effect or restricts the Due Process rights of employees and thus require no mitigation.

4d. Use of new technologies
The IFS application does not use new technologies and therefore has no effect or restricts the Due Process rights of employees and thus require no mitigation.

How are the effects to be mitigated?
There are no effects that would require mitigation.

Maintenance of Administrative Controls

1a. Explain how the system and its use will ensure equitable treatment of taxpayers and employees.
All activities of users within IFS are audited and reviewed to ensure equitable treatment of employees. By security and privacy training requirements being an annual assessment by all IRS system users; the continuous awareness of legislation, IRS policy, and IT practices are reviewed by all IRS employees to ensure awareness. The unauthorized or unethical use of any IRS data is strictly prohibited by IRS management, and all security incidents are investigated by the IRS.

1b. If the system is operated at more than one site, how will consistent use of the system and data be maintained in all sites?
Authoritative IFS data is maintained at the IRS ECC-DETROIT location and the primary IFS application servers are operated only at the ECC-DETROIT data center. The IFS Disaster Recovery (DR) is located in ECC-Memphis. Data replication between ECC-Detroit and ECC-Memphis occurs every six hours to ensure data and system consistencies between the two sites.
.

1c. Explain the possibility of disparate treatment of individuals or groups
None, IFS business rules, processes and designed capabilities is not configured or capable of causing disparate treatment of individuals or groups. All current IRS policies, practices, and procedures ensure that equal and fair treatment of all employees is enforced as an ongoing activity. Therefore, the probability of disparate treatment to any individual or group from the currently listed IFS capabilities is unlikely.

2a. What are the retention periods of data in this system?
IRM 1.15.36, Records Management, Records Control Schedule for Finance—Chief Financial Officer requires that financial records data be retained for at least 7 years and 1 months after the funds have expired.

Note: *All PII data within IFS, regardless of the associated connection, is retained for a minimum of 7 years 1 months. Due to the structure of the relational database, PII data elements are a shared information repository and not a distributed or replicated model. 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.*

2b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?
IFS complies with *IRM 2.7.4.4* (05-30-2003) Purging of Sensitive but Unclassified (SBU) Data and Destruction of Computer Media. The implemented IFS solution is presently four years old. By IRS guidance, all records are maintained for a period of 7 years 1 month. All IFS data currently resides within the IRS SAN repository and due to the life cycle value of the IFS solution, no data has been purged or archived from the system as of this filing.

Note: *All PII data within IFS, regardless of the associated connection, is retained for a minimum of 7 years 1 months. Due to the structure of the relational database, PII data elements are a shared information repository and not a distributed or replicated model. 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.*

2c. While data is retained in the system, what are the requirements for determining if data is accurate, relevant, timely, and complete to ensure fairness in making determinations?
IFS receive data inputs from trusted external sources to ensure that business processes for the IRS are based on “source data” feeds. The accuracy of this data is ensured by ISA and MOU agreements in place with IRS trading partners. By those agreements, the data provided by these sanctioned interfaces are considered approved IRS authoritative source that ensures that the data is accurate, timely and complete data. Electronically, the IFS system has an implementation of checksum and trigger file parameters to ensure that only complete file transfers are processed. Accuracy of business processes is ensured by generally accepted accounting rules for account reconciliation and year-end reporting.

3a. Is the system using technologies in ways that the IRS has not previously employed?
No, the IFS application is not using technologies that the IRS has not previously used.

3b. How does the use of this technology affect taxpayer/employee privacy?
The IFS application does not use any technologies not previously employed by the IRS and therefore has no affect on employee/taxpayer privacy.

4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
No, the IFS application does not have the capability to identify, locate and monitor individuals.

4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

No, the IFS application does not have the capability to identify, locate and monitor groups of people.
4c. What controls will be used to prevent unauthorized monitoring?
The IRS enterprise network provides intrusion detection systems to prevent unauthorized users or attacks on its systems. IFS is available to users on a “need-to-know” basis. Only those users with the requirement to view employee name and address information are assigned a role with these type of viewing privileges. The implementation of user profiles and authentication credentials (such as user

IDs and passwords) are used to prevent unauthorized personnel from accessing and/or viewing sensitive data elements. What the user sees on his or her computer screen, as well as in files, applications and directories is determined by how the user profile is set up.

5a. Under which Systems of Record notice (SORN) does the system operate?
Treasury/DO .210--Integrated Financial Management and Revenue System, last published in its entirety on August 31, 2000, at 65 FR 53085, is designated as "Treasury .009" and is being renamed as "Treasury Financial Management Systems".

- The following URL is the centrally controlled repository for U.S. Government SORNs, http://a257.g.akamaitech.net/7/257/2422/01jan20081800/edocket.access.gpo.gov/2008/E8-4430.htm.

5b. If the system is being modified, will the SORN require amendment or revision?
No.

View other PIAs on IRS.gov