DEPARTMENT OF TREASURY
Washington, D.C. 20220

HR Connect, Privacy Impact Assessment (PIA)

May 1, 2008

A. Identification

System Name: HR Connect
OMB Unique Identifier: 015-00-01-13-01-1226-24
System Owner: Treasury, Office of the Deputy Assistant Secretary for Human Resources/Chief Human Capital Officer (DASHR/CHCO)

Contact	Program Manager	Debra Vess
	Information System Security Manger	Renee Wilmot
	System Owner	Erik Johnson
	Privacy Act Officer:	Dale Underwood

Address:
FOIA/PA Request
Disclosure Services
Department of the Treasury
Washington, D.C. 20220

Telephone: (202) 622-0874
Fax: (202) 622-3895

B. System / Application General Information

1. Does the system contain any information in identifiable form (IIF)?

   Yes

2. What is the purpose of the system / application?

   HR Connect is Treasury's enterprise system, a web-based solution built on PeopleSoft commercial-off-t he-shelf (COTS) software. HR Connect transforms core back-office HR functions, moving them from a processing-centric capability supported by Treasury and National Finance Center (NFC) legacy systems, to a strategic-centric capability enabled through its commercial software underpinning. Additionally, self-service components of the software fundamentally transform the standard government HR service delivery model, putting additional information, services and processes (i.e., personal data, position management, requests for *personnel action, recruitment, reporting, etc.) directly in the hands of managers and employees.*

From a business perspective, Treasury's implementation methodology for HR Connect has mandated that all Treasury bureaus co-exist in one standard software code line, ending a Treasury history of bureau HR system autonomy through varied implementations of NFC and other legacy systems. Through HR Connect's implementation, HR and information technology standardization is being realized. Key Accomplishments/ Status: Treasury has been approved as an HR Line of Business (LoB) Shared Service Center (SSC). HRCPO anticipates that the LoB designation will help expand the current customer base and offer economies of scale that will reduce the cost per employee across the federal marketplace. Roughly 144,000 employees currently rely on HR Connect for their HR & payroll needs, including all of Treasury as well as HUD, DHS, and ATFE (which are cross-serviced by HR Connect under the HR LoB initiative).

Near Term Delivery Model - HR Connect supports the common HR LoB processes and provides core HR functionality that is interoperable, portable and scalable. Through partnership, HR Connect delivers components of long term HR LoB functionality today. HR Connect's core functions include: Administering Benefits, Managing Payroll, Personnel Action Processing, Time and Attendance and Labor Distribution.

3. What legal authority authorizes the purchase or development of this application / system?

   5 U.S.C. 301; Department regulations for the operations of the department, conduct of employees, distribution and performance of its business, the custody, use, and preservation of its records, papers, and property.

   31 U.S.C. 321; General authorities of the Secretary establishes the mission of the Department of the Treasury.

   e-Government Act of 2002 (H.R. 2458/S.803) supports government to government services. http://www.whitehouse.gov/omb/egov/g-4-act.html

4. Under which Privacy Act System of Record Notice (SORN) does this system operate?
   The SORN describes the HR Connect purpose, identifies participating customers, and type of services provided.

   Treasury .001--Treasury Payroll and Personnel System
   http://www.treas.gov/foia/privacy/issuances/treasurypa.html

C. Data in the System

1. What categories of individuals are covered in the system?

   Employees, former employees, and applicants for employment, the Treasury Department bureaus and offices and other Federal agencies that are customers of the HR Connect Program.

2. What are the sources of the information in the system?

   a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

      The information starts with the specific individual and is maintained in Systems of Records published via Treasury, its bureaus or other agency SORN. These Systems of Records comprise a databases and files that Treasury, its bureau's and other agencies maintain on employees for completing personnel actions. This information includes employee identification and status data such as name, records that establish an individual's identity, social security number, date of birth, sex, race and national origin, awards received, work schedule, type of appointment, education, training courses attended, veterans preference, and military service.

   b. What Federal agencies are providing data for use in the system?

      Personnel information data is provided by the Treasury Department, Housing and Urban Development (HUD), Department of Justice (DOJ), and Department of Homeland Security (DHS). Other supporting data is provided by the Department of Defense (DOD), Office of Personnel Management (OPM), Social Security Administration (SSA) and DOL.

   c. What State and/or Local agencies are providing data for use in the system?

      State unemployment commissions provide information that is categorized into specific system of records that are compiled for use in the US Treasury and bureau specific human resource information.

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

      Third party information source data collection is limited by the statutory prerequisites for purposes of obtaining employment within the Department of the Treasury and its bureaus and other Federal agencies who utilize HR Connect. See 2A, collection is limited under title 5.

   e. What information will be collected from the employees, government contractors and consultants, and the public?

There is no information collected from the public or from government contractors and consultants for this system.

The employee information collected comes directly from the individual employee or from a source designated in writing by the employee.

3. Accuracy, Timeliness, and Reliability

   a. How will data collected from sources other than Treasury records be verified for accuracy?

   Any data that is collected from sources other than HR Connect records concerning an employee is subjected to the data protections afforded by the Privacy Act of 1974, as Amended [5 USC 552a].
   Verified for accuracy, employee review and agency HR Specialist through application data management business rules. This is specifically verified through SF50 functionality.

   b. How will data be checked for completeness?

   The data must conform to the Privacy Act protections under 5 USC 552a. The data completeness will also be checked for accuracy and relevancy. The data will be checked for completeness through the application of data management business rules which require the employees to review the SF-50 annually.

   c. Is the data current?

   Data comes directly from the individual. Data obtained on individuals from other sources are from sources specified by the individual. The currency of the data from third parties is subject to the third party's data management business rules.

   d. What steps or procedures are taken to ensure the data is current and not out-of-date?

   The HR Connect system permits the individual to update their data throughout their employment to keep it current. The currency of the data obtained from third parties is subject to the third party's data management business rules.

   e. Are the date elements described in detail and documented?

   Yes, all data elements pertaining to human resource information have been detailed and documented pursuant to the requirements imposed by OMB Circular A-130. The name of the document is the HR Connect Requirements Model Plan. Additionally, all of the data elements are known *as part of the documentation requirements imposed by the Treasury Information Systems Life Cycle (ISLC) management and the configuration management procedures being adhered to by Treasury.*

D. Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is designed?

   Yes

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? If so, how will this be maintained?

   No, to the derivation of data and, yes to the creation of previously unavailable data. HR Connect will not derive new data since it is a replacement system on an enterprise scale for the Department of the Treasury human resource information. Therefore, there is one piece of data creation that is previously unavailable data. That is, the system generated employee identifier data. However there is no aggregation that is being collected from the information since the source of the information is from the individual. This individually supplied data is being used to populate the system known as HR Connect and this data originates with the individual supplying the information for data collection.

3. Will the new data be placed in the individual's record?

   Yes. The employee identifier number will reside within HR Connect and will be used to identify the employee to the system as long as the individual remains with the Treasury Department or one of its bureau's or customer agencies.

4. Can the system make determinations about employee/public that would not be possible without the new data?

   The system makes determinations about employees through utilization of competencies that are presently being used in the manual personnel selection procedures for promotion/career ladder accessions. No determination will be made based on new data.

5. How will the new data be verified for relevance and accuracy?

   If any new data originates with the individual supplying the information except for the system generated employee identifier. Verification for relevancy and accuracy inures to the individual as it pertains to their own Personally Identifiable Information (PII).

6. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

   Any data consolidation that occurs is protected under statutory controls, such as the Privacy Act, configuration management controls, security controls, profiles and access controls in conjunction with the "need-to-know" principles for data protection.

7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?

   Yes. Under the configuration management and data controls that are currently in place for HR Connect, only authorized individuals may access their own personally identifiable information under the "need-to-know" authorities. The proper controls remain in place to protect the data and prevent unauthorized access. HR Connect complies with Treasury IT security policy for certification and accreditation, risk assessments and continuous monitoring of security controls.

8. How will the data be retrieved? Does the personal identifier retrieve data? If yes, explain and list the identifiers that can be used to retrieve information on the individual.

   Yes, data is retrievable by personal identifier. Data can be retrieved either by the employee identifier as it pertains to an individual, or by the name of the employee if the information is being retrieved by the manager of record.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

   HR Connect has numerous reports built into its system and data is also defined in HRRPT. Employee related data is available to managers for effective workforce administration; for example the processing of personnel actions, roster, employee location, not-to-exceed (NTE) dates, emergency contacts, pending and processing actions, and financial disclosure.. Included in HR reports are inbound interface reports, NFC error listings (SINQ), manager initiated actions, group/mass awards, NTE dates, emergency contacts, etc. HRRPT is an ad hoc reporting tool which includes information on the employee, job, position, and performance related information.

E. Maintenance and Administrative Controls

1. If the system is operated in more than one site, how will the consistent use of the system and data be maintained in all sites?

   The Treasury Department HR Connect is operated at a single location, the Federal Data Center, which is currently located at the Detroit Computing Center.

2. What are the retention periods of the data in the system?

   The retention periods of data contained in this system are covered by General Records Schedules #1, Civilian Personnel Records and have various retention periods for specific types of data.

3. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

   Reports in the system are retained for 7/14 days based on data management business rules.
   The procedures for eliminating the data at the end of the retention period adhere to the Federal Records Act of 1950 and National Archives and Records Administration guidelines in addition to the Treasury Information Systems Life Cycle (ISLC) management requirements.

4. Is the system using technologies in ways that Treasury has not previously employed (e.g., monitoring software, smart cards, caller-ID)?

   HR Connect is a integrated Treasury Department owned and operated human resource enterprise solution that is using a proven COTS product supported by technology that has a well established reputation.

5. How does the use of this technology affect public/employee privacy?

   The technology will enhance an individual's control over their own Personally Identifiable Information (PII) through role based access.

6. Will this system provide the capability to identify, locate, and monitor individuals?

   HR Connect does provide the capability to identify an employee via the employee identifier to gain access to the system through the network gateway. It also provides the capability to locate and authenticate an individual to ensure that only authorized individuals are utilizing the system. The monitoring capabilities are a security requirement in order to ascertain whether or not an individual is *attempting to thwart the security mechanisms or manipulate data that is not owned by the individual nor access permissions under "need-to-know" principles.*

7. What kinds of information are collected as a function of the monitoring of individuals?

   Currently, HR Connect is collecting the ID, time, date, successful logins and failed login attempts for both privileged and non-privileged users.

8. What controls will be used to prevent unauthorized monitoring?

   HR Connect has, built into the system, security checks in order to ensure that privacy safeguards are not abused or bypassed. For instance, access profiles are used to enable an individual to access their own information but will permit security administrators to monitor any individual that engages in any unauthorized or malicious behavior within the HR Connect environment. In addition, before users complete registration they must accept the system Rules of Behavior. Audit trails are reviewed on an ad-hoc bases and monitoring tools such as intrusion detection devices and vulnerability scanning tools have also been deployed

9. Under which Privacy Act SORN does the system operate?

   The System of Record Notice is: Treasury .001--Treasury Personnel and Payroll System

10. If the system is being modified, will the Privacy Act SORN require amendment or revision?

    No.

<u>F. Access to Data</u>

1. Who will have access to the data in the system?

   Department of the Treasury and Customer Agency Employees and Managers. HR Connect System Administrators, Developers, and system maintenance personnel at the Federal Data Center located at the Detroit Computing Center. All access is based on "need to know" and the corresponding system access profiles.

2. How is access to the data by a user determined?

   Access to the data by a user is determined based upon the user profile that is determined under the strict "need-to-know" criteria and also as a function of position. The criteria, procedures, controls, and responsibilities regarding access are documented in the security features user guides. .

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

   Users will only have access to the data that is inherently theirs to access such as their own Personally Identifiable Information (PII). In the case of managers, these managers will only have access to the information that is specifically under their direct ownership or strict "need-to-know" access controls [i.e., employees assigned to them] as well as, their own personally identifiable information.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

   Entrances to data centers and support organization offices are restricted to those employees who require access. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols, which are periodically changed. (Every ninety days a password change required). In addition privilege users are required to annually sign the rules of behavior. (An electronic copy of the rules of behavior is available on the HRConnect system)

   The HR Connect application prevents the misuse of the data through a profiled access approach. That is, only individuals with an established "need-to-know" may access only their specific profiled data that is controlled by the system security mechanisms that are outlined in NIST 800-53 and the HRConnect system security plan.

5. Are contractors involved with the design and development of the system and will / are contractors involved with maintenance of the system?

   Yes When a contract provides for the operation of a SOR on behalf of the Department, the Privacy Act requirements and Departmental regulations on the Privacy Act must be applied to such a system The Federal Acquisition Regulations (FAR) also require that certain information be included in contract language and certain processes must be in place (see FAR 48 CFR.24.102(a) and Treasury Acquisition Regulation 48 CFR.

6. Do other systems share data or have access to the data in the system? If so, explain.

   Yes, shared with the data owners but not unauthorized third party organizations and companies. As HR Connect is presently configured, other systems are not sharing data contained in HR Connect. HR Connect is the data store for human resource information under Treasury member bureau and HRLOB customer auspices. As such, any system wishing to have extracts from HR Connect must follow configuration management principles and procedures in conjunction with the HR Connect Program Office and member bureau's and agencies prescribed *information systems protocols to have access to HR Connect via specific written agreement. The data is inserted into other systems and then sent to HR Connect.*

7. Who will be / is responsible for protecting the privacy rights of the public and employees affected by the interface?

   All users of the HR Connect system are responsible for protecting privacy rights of employees. This is communicated through security and privacy awareness training on an annual basis. For the interfaces described above, the HR Connect System Owner and the Information Owner of the data involved in the interface is responsible for protecting the privacy rights of the employees affected by the interface.

   As previously stated, the interface as used in this context is not occurring at the present time. However, should any such interface surface or occur to support future releases or functionalities within HR Connect, the responsible party or parties for protecting the privacy rights of employees will reside with each individual who has access to their own personally identifiable information and ultimately the Treasury secretary as well as his/her agency counterparts as the owner and users of the HR Connect enterprise system. In the case of HR Connect, the support staff who may have access to information that is generated from any potential future interface would also be responsible for protecting the privacy rights of individuals.

8. Will other agencies share data or have access to the data in this system (e.g., Federal, State, Local, other)?

   Other non-customer agencies may provide data on specific individuals at their request to the Treasury Department’s HR Connect. As such, those agencies may share data but will not have access to the data in the HR Connect system.

9. How will the data be used by the other agency(s)?

   Data is only shared under statutory authorities/dictates mandated under the Privacy Act and Treasury Department policies. The agency that receives information must adhere to the statutory dictates under which the information was supplied to them. The agency is provided access through role based access control.

10. Who is responsible for assuring proper use of the data?

    The data providers are responsible for assuring proper use of the data through various agreements and statutory mandates [i.e., the Privacy Act].