DEPARTMENT OF TREASURY
Washington, D.C. 20220

Entry on Duty System (EODS)
Privacy Impact Assessment (PIA)

July 2010
Version 1.0

System Information

System Name: Entry on Duty System (EODS)
OMB Unique Identifier: 015-00-01-13-01-1261-24

Contact Information

1. **Who is the person completing this document?**
   Gladys Wiggins
   Project Manager
   1750 Pennsylvania Avenue, NW
   Washington, D.C. 20220
   (202) 622-3685
   Gladys.Wiggins@do.treas.gov

2. **Who is the system owner?**
   Erik Johnson
   Assistant Director Systems Development Division
   1750 Pennsylvania Avenue, NW
   Washington, D.C. 20220
   202-927-5604
   Erik.Johnson@do.treas.gov

3. **Who is the system manager?**
   Debra Vess
   Associate Chief Information Officer for the HR Connect Program and
   EODS Information Owner 1750 Pennsylvania Avenue, NW
   Washington, D.C. 20220
   (202) 927-5289

   Debra.Vess@do.treas.gov
4. **Who is the Information Systems Security Manager who reviewed this document?**
   Renee Wilmot
   Information System Security Manager
   1750 Pennsylvania Avenue, NW
   Washington, D.C. 20220
   (202) 622-5346
   Renee.Wilmot@do.treas.gov

5. **Who is the Bureau Privacy Act Officer who reviewed this document?**
   Dale Underwood
   Privacy Act Officer
   1750 Pennsylvania Avenue, NW
   Washington, D.C. 20220
   (202) 622-0874
   Dale.Underwood@do.treas.gov

System Application/General Information

1. **Does this system contain any information in identifiable form?**

   Yes

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

   The EODS is an Internet-Facing application that services newly hired federal employees before they begin their employment at a federal site. EODS provides an automated on-boarding process that focuses on pre-employment on-boarding benefits forms completion and data collection and delivery of new hire information to prospective federal employee. The system is an independent application and receives limited (position) data from its interface with the *HR Connect* application which serves as the Treasury Department's Human Capital Management system and an Office of Personnel Management (OPM) approved federal HR Line of Business.

   The public-facing Internet portion allows EODS applicants to access their information via SSL across the internet. The intranet portion, also via SSL, allows HR Specialists to administer and track applicants' benefits package completion and the interconnection between EODS and HR Connect.

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

   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 for the Secretary establishes the mission of the Department of 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 SORN does the system operate? (Provide the system name and unique system identifier.)**

   System Name: Entry on Duty System (EODS)
   Unique System Identifier: 015-00-01-13-01-1261-24

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

Data in the System

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

The categories of individuals consist of new employees, former Federal employees, and current Federal employees who seek government employment.

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?**

   Information concerning candidates and employees in the system is collected from the individual or HR Specialist via electronic forms.

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

   At this time, no Federal agencies will be providing data for use in the system.

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

   None.

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

   None.

   e. **What information will be collected from the employee and the public?**

   Information collected is from an applicant who has received a job offer for Federal employment (until they are actually hired, applicants are viewed as the 'public') complete onboarding package, including Individually Identifiable Information (or Personally Identifiable Information (PII)) e.g.; home and contact information, race, citizenship, benefits, medical, tax, financial, etc..

3. **Accuracy, Timelines, and Reliability**

   1. **How will data collected from sources other than bureau records be verified for accuracy?**

   Data is collected directly from the individual. Accuracy is verified by both the individual upon submission into the EODS and the HR Specialist.

   2. **How will data be checked for completeness?**

   Data is checked for completeness by system edits, the individual and the HR Specialist.

3. **Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models.)**

   Data is current as of the date it is collected. Data verification is conducted by the employee or applicant and the HR specialist.

4. **Are the data elements described in detail and documented? If yes, what is the name of the document?**

   Yes, all data elements pertaining to EODS have been detailed and documented pursuant to the requirements imposed by OMB Circular A-130. The documents include; the *EODS Requirements Specification*, July 23, 2009, and the *EODS Data Model.* Integration between EODS and eOPF is planned for FY2011.

Attributes of the Data

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

   Yes.

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

   No, the system will not derive or aggregate any new data about the individual from the data entered by the individual applicant. While any data resides in EODS it will be maintained pursuant to the requirements imposed by OMB Circular A-130 Appendix III, the Privacy Act, and FISMA[1].

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

   Not applicable, since no new data is derived about the individual applicant.

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

   The system does not make determinations about the data however; system edits are performed to enhance the data collection process. These edits support completeness.

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

   Verification for relevancy and accuracy is performed by the individual or applicant and the HR specialist.

[1] Federal Information Security Management Act of 2002 (FISMA) P.L. 107-347 (Title III of the E-Government Act 0f 2002)

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

   Data is not being consolidated. All system data is protected under statutory controls, such as the Privacy Act, configuration management controls, FISMA security controls, encryption at rest and in transit, and permissions are granted through Role-Based 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? Explain.**

   Processes are not being consolidated. A risk assessment has been conducted as part of the security certification and accreditation. The system contains appropriate controls to enforce system security, system quality assurance and system integrity. Annually, controls will be validated according to FISMA reporting requirements.

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

   Yes, data is retrievable via personal identifier; the applicant/employee's name, but not by social security number (SSN).

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

   Two reports will be generated based on data from EODS; 1) EODS Report and 2) New Hire Benefits Report. The EODS Report provides the list of on-boarding employees with the same EOD date, to notify of employees' impending arrival. The New Hire Benefits Report provides summary information on new hires' benefits elections. These reports will be accessible to HR specialist.

Maintenance and Administrative Controls

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

   The EODS is operated at a single location in Macon, GA at a federal data facility. The contingency site for EODS is in Boyers, PA. A data synchronization tool will keep data in synch between primary and backup sites for Disaster Recovery (DR) purposes and data consistency.

2. **What are the retention periods of data in this 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. The system complies with the Department of Treasury *Directive 80-50*

Records and Information Management Manual. In accordance with TD 80-50, records are not destroyed or otherwise alienated from the system except in accordance with procedures prescribed in 36 CFR, Part 1228.

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 are generated on an ad hoc basis based through standard queries and are deleted when not being used. Individual reports may be saved by HR Specialists independent of the system. CSAT Training is provided to all federal users instructing them to dispose of sensitive data properly. 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 and OMB Memorandum M-06-16 *Protection of Sensitive Agency Information* (data extracts including sensitive data are erased within 90 days).

4. **Is the system using technologies in ways that the bureau/office has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

   The new Internet-accessible EODS is a proven web-based COTS product supported by technology that has a well established reputation.

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

   The supported technology will provide a layered protection defense through Role-Based Access Controls (RBAC) and data encryption for sensitive data.

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

   EODS 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 provide up front situational awareness and enhances IT asset protection to avoid system or data compromise. Additionally, EODS includes system performance tools for monitoring system performance.

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

   EODS collects ID, time, date, successful and failed login attempts for both privileged and non-privileged users.

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

   EODS has built-in 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 administrators to monitor any individual that engages in any unauthorized or malicious behavior within the EODS environment. In addition, before users' complete registration they must accept the system Rules of Behavior. Audit trails are reviewed on a quarterly basis 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? Provide number and name.**

   (*See also question 4, page 4.)* Treasury .001--Treasury Personnel and Payroll System; http://www.treas.gov/foia/privacy/issuances/treasurypa.html.
   This SORN addresses the EODS system capabilities and objectives.

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

    EODS is a newly developed system, and these functions are covered in the existing SORN and do not constitute a significant change.

Access to Data

1. **Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others.)**

   a. Applicant (public)
   b. Employee
   c. HR Specialist
   d. Database Administrator
   e. System Administrator

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

   Access to the data by a user is 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 System Security Plan. The Department of the Treasury IT Security Program Directive 85-01 (TD P 85-01) clearly documents that the system manager is responsible for ensuring that access to the information and data is restricted to authorized personnel on a need-to-know basis.

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

   Access will be restricted through role-based access controls. 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 HR Specialists, they will only have access to the information that is specifically under their direct ownership or strict "need-to-know" access controls 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? (List processes and training materials.)**

   Entrances to data centers and support organization offices are restricted to those employees who require access. Disclosure of information through IT assets is restricted through the use of passwords and sign-on protocols, which are periodically changed. All users are required to sign the rules of behavior each time they log into EODS.

   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 EODS system security plan. The EODS system meets compliance with NIST and Treasury Security policies, and implements the full level of controls for a Moderate system, as documented in the EODS System Security Plan (SSP).

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other statutory and regulatory measures addressed?**

   For the design and development of EODS, contractors will be utilized. Contractor will also provide O&M services. Yes, Privacy Act contract clauses were inserted in their contracts per FAR[2] 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 yes, explain.**

   No other systems share data with EODS at this time. However, EODS data will be integrated with the Electronic Official Personal File (eOPF) in the future.

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

   All users/applicants are responsible for data protection as outlined in the EODS Rules of Behavior (RoB); however the information owner, and ultimately the System Owner and Authorizing Official have the responsibility to see that the data is protected from all threats.

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

   No other agencies share data with EODS at this time.

9. **How will the data be used by the other agency?**

   This question is not applicable.

[2] Federal Acquisition Regulations (FAR)

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

The EODS Authorizing Official (AO), the Associate CIO, is accountable for EODS security. Data providers are responsible for assuring proper use of the data through various agreements and statutory mandates [i.e., the Privacy Act]. The individual applicants, as data providers, are responsible to ensure the data entered is correct.