Privacy Impact Assessment
for the

Personnel Locator System

Environment and Natural Resources Division

July 2007

Contact Point
Donna Whitaker
ENRD Executive Office
Office of Information Management
202-616-3100

Reviewing Official
Kenneth Mortensen
Acting Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 353-8878

Introduction

The Environment and Natural Resources Division (ENRD), Department of Justice, is designing a new system of records to store personnel locator information. The Personnel Locator System (PLS) will include modules with locator information (including professional background held by particular staff) as well as emergency contact information. Managers and staff desire to locate all of this information in a centralized, searchable database to simplify system maintenance, and more efficiently maintain accurate timely, and consistent information.

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

The general locator portion of the Personnel Locator System will contain records filed by name of employee or affiliated personnel, including his or her position title; office location; office telephone and facsimile (fax) numbers; office address; professional electronic mail (email) address(es); and optional photograph. The locator information will also include records filed by name of employee or affiliated personnel concerning professional backgrounds and expertise, including any self-declared experience, skill or certification in the following areas: law school name and year(s) of graduation; clerkships; bar memberships; advanced degrees earned; foreign language expertise; and Notary Public commission.

The emergency contact information module of the Personnel Locator System will contain comprehensive contact information from employees or affiliated personnel that may be used to contact the person named, or his/her authorized designee, in the event of an emergency during or outside of official duty hours. Information categories include home addresses and telephone numbers; cellular telephone numbers; pager numbers; other alternate telephone numbers where persons or their designees may be reached while away on travel, assigned work detail, or other extended absence from the office; electronic mail (email) addresses; names, telephone numbers and email addresses of family members or other emergency contacts; and other emergency contact information persons may wish to provide.

1.2 From whom is the information collected?

Information will be collected from Employees, Student Aides, Law Clerks, Volunteers, Contractors and other personnel employed by or otherwise affiliated with the Environment and Natural Resources Division, U.S. Department of Justice. Participation is voluntary; personnel may provide all, some or none of the requested information.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

Division personnel collaborate on cases and matters requiring specialized legal expertise and often require assistance from colleagues with particular background or skills. The ENRD staff desires a centralized, searchable directory of employee expertise with associated locator information to facilitate professional contacts. ENRD desires to maintain its emergency contact database in the same system of records to assist with the ease of data entry and information updates for or by employees, and to simplify system maintenance for the Information Technology (IT) administrators.

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

Division personnel will access the database to:

- Identify colleagues with knowledge and/or expertise that may be helpful with work on a particular case or project (e.g., a foreign language expertise that is needed for document translation)
- Review employee photographs to assist with recognition of colleagues at meetings or in other professional settings
- Contact employees or their designees with situational information during Continuity of Operations (COOP) activation or other emergencies (authorized employees only)
- Use photographs to assist with identification of employees, if necessary, in the event of a catastrophic event onsite during official duty hours; and use personal information to get in touch with designated emergency contact persons (Office of Human Resources or COOP Action Officers only)

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

Information will be available to ENRD personnel via the ENRD Intranet (ENRDNet). The information will not be shared with other internal components of the Department.

Section 5.0
External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

Information will be available to ENRD personnel via the ENRD Intranet (ENRDNet). The information will not be shared with external (non-DOJ) recipients, unless specifically requested under an exception allowed by the Privacy Act of 1974, in which case the requested data will be released accordingly.

Section 6.0
Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Participation is voluntary. Individuals will be invited to input information into the database. At their option, they may choose to input all, some, or none of the requested information. Participants are informed that their participation is voluntary and that no penalty will ensue from non-participation. The

system is designed so that individuals can also change their decision and select and/or unselect any module at any point in time.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Onscreen notices inform participants of the purpose of data collection and the specific uses of the information. Participants are asked to expressly consent to the use of the information they provide for the purposes that are listed onscreen. This consent, or permission, is given in electronic form by each individual when he/she selects (or un-selects) a check-box button accompanying an on-screen statement of permission.

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

ENRD users of the Justice Consolidated Office Network (JCON) will have access to the application. All users will have the same access to the locator and expertise information on the database. Access to personal contact information will be restricted according to types of users. For this purpose, users are classified into the following groups: (1) COOP Leadership Teams (including offsite relocation deployment team); (2) COOP Action Officers (CAOs); (3) Travel Program Manager; (4) Section Management Teams; (5) Office of Administrative Services and Support Services Contract Project Managers (Office of Administrative Services); (6) Office of Human Resources; (7) JCON users.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Contractors with ENRD JCON accounts will have access, including, but not limited to, contractors who support the following Division functions: (1) Comprehensive Support Services (mail, fax, filing, copy services, records management); (2) Litigation Support; (3) Database/Systems Support; (4) IT Help Desk; (5) IT Server Deployment; (6) Financial Administration. Appropriate sections of the contracts governing their access to Division data and responsibilities to safeguard those data are attached.

8.3 Does the system use "roles" to assign privileges to users of the system?

All employees with access to PLS will be able to view information in the locator portion of the system (office location, etc.), as well as the accompanying employee photographs (when permission is given to post a photograph), but only system administrators will be able to edit these records. There are no specialized "roles" designating other viewing or editing privileges in this section.

Each participating employee will be able to enter data into the record pertaining to his/her own professional background and expertise. All employees will be able to view all of the records from this section of the database. No additional specialized "roles" are needed for this module of PLS.

Access to the personal information in the emergency contact (COOP) section of PLS is restricted according to designated authority in a COOP situation. "Roles" are assigned using the categories listed in Section 8.1 of this document. These roles allow the following privileges:

(1) *COOP Leadership Teams (including offsite relocation deployment team)*: Allowed to update own record and view records of all Division personnel;
(2) *COOP Action Officers (CAOs):* Allowed to update own record, may view and update records of personnel under his/her span of control;
(3) *Travel Program Manager:* Allowed to update own record and view records of entire Division;
(4) *Section Management Teams:* Allowed to update own record, may view and update records of personnel under his/her span of control;
(5) *Office of Administrative Services and Support Services Contract Project Managers:* Allowed to update own record, may view records of entire Division;
(6) *Office of Human Resources:* Allowed to update own record, may view records of entire Division;
(7) *JCON users:* Allowed to update own records.

During a COOP situation, only 11 ENRD leadership personnel will be co-located in alternate work space. All other ENRD personnel will be expected to work from remote locations. The *COOP Leadership Teams* will have access to all records so that they may be in contact with whichever personnel are needed to continue government business or restore normal operations.

The *Office of Administrative Services* will have access to all records so that mail and packages can be rerouted to personnel according to the personal location that is specified in their records. If, during an emergency, personnel are working from a different location than that originally specified in their record, they may update the record themselves (*JCON Users*) to reflect the new information, or the *CAO* or *Section Manager(s)* assigned to them can do it for them if they are unable to access the application from their location.

The *Office of Human Resources* will have access to all records so that HR staff can handle family notifications efficiently in the event that a catastrophic emergency occurs during business hours. The *Travel Program Manager* has access to all records so that he/she may contact employees or their families to assist with travel arrangements for personnel who may be away from home when an emergency occurs,

or with making travel arrangements for the *COOP Leadership Team* or other personnel when relocation to a secondary or tertiary site becomes necessary. In ENRD's COOP plan, those sites are in our Western Field Offices.

8.4 What procedures are in place to determine which users may access the system and are they documented?

For accessing personal contact information, which is restricted according to authorization, "roles" are assigned using to the categories listed in Sections 8.1 and 8.3 of this document.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

These roles first were defined, and persons assigned to them, in the ENRD COOP Plan. The assignments are verified and updated periodically according to requirements of the COOP program. For the emergency contact section of PLS, business rules have been written to document these roles and privileges. Access privileges will be updated or revised as notice is given of personnel changes, and also will be verified against the list of current COOP personnel twice each year when the designations of those roles and assignments are reviewed, as required by regulation.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Information in this system is appropriately safeguarded with physical and technical protections. Information will be stored electronically in a database located on a server connected to the Division's intranet. Access to the information is limited to persons with access to ENRDNet, and certain information is further restricted to those with a need to know for the performance of official duties.

Information access will be governed by security safeguards as described below:

(1) General locator information: Data editors will be restricted to ENRD Executive Office personnel, contractors, and other affiliated staff. All ENRD personnel may view these records in read-only format.

(2) Professional background information (expertise): Each staff member may edit his or her own record to keep information accurate and current. Personnel may not edit records other than their own. System administrators will have full editing privileges over these records. Other ENRD personnel may view these records in read-only format.

(3) Emergency contact information: Each person will be able to view and edit his or her own emergency contact information record so that he or she may keep this information accurate and current. ENRD emergency coordinators and managers will have editing rights according to level of responsibility so that they may update these records on behalf of staff, if necessary, during emergencies or as needed at other times. System administrators will have full editing privileges over these records. Viewing privileges will be restricted to managers and certain other employees or contractors with a need to know.

Technical equipment for the Personnel Locator System database is maintained in buildings with restricted access and is safeguarded in accordance with applicable rules and policies, including the Department's automated systems security and access policies.

Personal information and photographs will be used only with employee consent and therefore the privacy impact is minimal. The Personnel Locator System will record the last date the employee consented or declined to allow this information to be available and will save this audit trail. Additionally, an audit record will be saved each time emergency contact information is updated by someone other than the employee (an emergency coordinator, manager, or system administrator). This record will include the employee, changed field, old value, new value, date of change, and the individual making the update.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Information and procedures pertaining to the use and handling of data in the PLS database is provided to users within the application. ENRD's Law and Policy Section (LPS) is developing general privacy training for all ENRD staff to raise awareness of these important and complex issues.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The application will be a part of ENRD's JCON system and is secured under FISMA requirements accordingly. The most recent Certification and Accreditation (C&A) of ENRD's JCON system was completed in August 2005. OMB Circular A-130, Appendix III, requires that all Federal information systems processing sensitive information be accredited and that accreditation documents be reviewed at least every three years. ENRD will complete its review and revalidation of the JCON C&A accreditation documents before August 2008.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Minimal privacy risks were identified, given that access only is granted to users with ENRD JCON access, and access to the personal contact information is further restricted to those with a need to know. Persons with a need to know were carefully identified, their system roles and responsibilities have been documented, and audit trails have been put in place to identify changes/updates made by persons other than the primary individual identified in a record. Appropriate physical safeguards are in place, and the application is protected by the network safeguards in place for the JCON system on which it is located.

Conclusion

The concluding section should inform the reader, in summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.

The PLS application was designed to collect certain personal information from ENRD staff that will be helpful to conducting business during normal operations, or necessary to conducting business during emergency operations. During database design, project team members made protection of privacy a paramount consideration, determining that only ENRD staff would have access to the database, only certain staff with a need-to-know would have access to the personal contact information collected for emergency use, and all privilege and access information will be well-documented.

Responsible Officials

Project Officer
Donna B. Whitaker
Director, Office of Information Management
Executive Office, Environment and Natural Resources Division
US Department of Justice

Privacy Officer
Peter J. McVeigh
Attorney
Policy and Legislation Section, Environment and Natural Resources Division
US Department of Justice

Approval Signature Page

_____/s/_____ ____7/3/08_____

Kenneth Mortensen
Acting Chief Privacy and Civil Liberties Officer
Department of Justice