Privacy Impact Assessment

Name of Project: Civilian Personnel Records-Office of Personnel Management Document Conversion Utility

Project's Unique ID: DCU

Legal Authority(ies): 44 USC 2108, 2110, and 2907

Purpose of this System/Application:

The Civilian Personnel Records-Office of Personnel Management Document Conversion Utility will store and transmit electronic copies of civilian official personnel files (OPFs). Civilian OPFs will be scanned into the system and these digitized files will be transferred to the Office of Personnel Management (OPM) Electronic OPF system.

The National Personnel Records Center (NPRC) has signed an agreement with the Office of Personnel Management to digitize and transfer civilian Official Personnel Files to the OPM electronic Official Personnel File (eOPF) system. Some of the OPFs pertain to former federal employees whose paper records are stored at the Civilian Personnel Records (CPR) Center and the rest pertain to current federal employees whose employing agencies have contracted with CPR to convert paper OPFs to digital format.

- The system is designed to provide a Production environment that will convert paper documents into digital formats using automated processes.

Section 1: Information to be Collected

1. Describe the information (data elements and fields) available in the system in the following categories:

Following are the categories of users that configure, operate, and maintain the CPR-OPM Document Conversion Utility system during normal use.

- **Administrators.** Members of the administrators group are the most privileged users in the system. Administrators have full access to all devices included in the system, including servers and network devices (firewalls, routers, switches, etc.)

  The positions occupied by the CPR-OPM Document Conversion Project Administrators group members are designated as ADP I (Critical Sensitive). All Administrators group members must have a NACI background investigation for system access. None of the CPR-OPM Document Conversion Project Administrators group members are permitted to be Foreign Nationals.

- **Power Users.** Members of the Power Users are limited privileged users. They will have full access to devices for which they are responsible, such as individual

workstations and shared servers, and read-only and/or read-write access to other resources as required by their job function.

The positions occupied by the CPR-OPM Document Conversion Project Power Users group members are designated as ADP II (Non-critical Sensitive). All Power Users group members must have a NACI background investigation for system access. None of the CPR-OPM Document Conversion Project Power Users group members are permitted to be Foreign Nationals.

- **Users.** Members of the User group are considered to be non-privileged users. They will have read-only and/or read-write access to individual resources as required by their specific job function. Access may also be limited by time, schedule, and location constraints, as defined by the overall system policy.

  The positions occupied by the CPR-OPM Document Conversion Project Users group members are designated as ADP III (Non-sensitive). All Users group members must have a NACI background investigation for system access. None of the CPR-OPM Document Conversion Project Users group members are permitted to be Foreign Nationals.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?

a. Employees

– User identifiers (user login ID) and authenticator (password)

b. Audit trail information (including employee log-in information)

Windows OS Audit Trails and Logging

All servers that are components of CPR-OPM Document Conversion Project are running Microsoft Windows Server 2003 Operating System. These operating systems are configured to audit the following information on the servers:

- Account Logon Events - both successful and failed account logon attempts are audited
- Account Management - both successful and failed attempts to manage (create, delete, edit) user accounts are audited
- Logon Events - both successful and failed logon events are audited
- Object Access - both successful and failed object access attempts are audited
- Policy Change - both successful and failed attempts to audit system policies are audited
- Privilege Use - failed attempts to privileged resources are audited
- System Events - both failed and successful system events are audited

Kofax Ascent Capture and Indicius Audit Trails

The Kofax Ascent Capture and Indicius software has auditing functions enabled within the application. This audit log captures all activities and events performed on the system by all Kofax users. These events and activities that are logged include logins/logoffs, batch information, user performed functions tracked, creation of batches and images within Kofax, account management activities, etc

Input/Output Controls
Audit trails are used for receipt of inputs/outputs from the information system. A record is kept of individuals who implement media disposal actions and individuals who verify that such information or media was properly sanitized. Inventory records of all storage media containing organizational information are maintained for purposes of control and accountability.

c. External Users – N/A

d. Other Federal agencies (list agency) - The records in the DCU system converts official personnel files into digital images. The original files belong to the Office of Personnel Management.

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.
The career of a federal civilian employee is documented by the long-term records found in OPFs. The OPF chronicles an individual's employment status, service, qualifications, benefits, rights, and employment history. OPFs are retired to the NPRC within 120 days after separation from Federal employment. Each data element in the OPF is necessary to document the career of the individual Federal employee.

Information concerning users of the system is necessary to ensure that there is controlled access within the system based on the performance of authorized tasks.

2. Is there another source for the data? Explain how that source is or is not used?

No.

Section 3: Intended Use of this Information

1. 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?

It is anticipated that there will be late-flowing documents that NPRC/CPR will receive from OPM. When this occurs, and it is determined that an eOPF already exists, the late-flowing documents will be scanned into the appropriate individual's eOPF. The paper documents will then be stored as "Dead Files" at NPRC/CPR.

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

Yes.

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

The system does not make determinations about the employees. Any determinations would be the responsibility of OPM.

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

That decision is made by OPM prior to sending the documents to NPRC/CPR.

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

Electronic OPFs, like paper OPFs, are protected under the Privacy Act. In addition, the employees who perform the scanning received NACI checks, underwent NARA IT Security Training, and are well-orientated as to the confidentiality requirements of their positions.

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

N/A

7. Generally, how will the data be retrieved by the user?

Authorized users can retrieve information by the full name and social security number (SSN) that the employee used during Federal employment. Other information in the system related to an individual include: date of birth; name of employing Federal agency; and beginning and ending date of Federal service.

8. Is the data retrievable by a personal identifier such as a name, SSN or other unique identifier? If yes, explain and list the identifiers that will be used to retrieve information on an individual.

Yes, OPFs in the system are retrievable by both name and social security number. Individuals seeking access to an OPF must provide the identifying information referenced in item 7 above, to assist us in locating a file. First party requesters receive a complete copy of the file upon request. Third party requesters may receive only the following information from an individual's OPF: position titles and occupational series, grades, annual salary rates, duty stations, and position descriptions for the present and the past.

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

The Document Conversion Unit (DCU) can generate productivity reports based on the OPFs/SSNs processed. The batch name has the SSN (of the subject of the converted OPF) embedded in it along with the Agency abbreviation and Batch iteration.

Only the Supervisor, support personnel and Lead Technician have access to these reports.

The Document Conversion Utility does not create reports about the subject of each OPF record.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.

Yes. NARA can make a distinction between first and third party requesters who are seeking access to OPFs in the system.

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain.

No

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

N/A

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

CPR-OPM Document Conversion Utility system and its users are subject to NARA-wide input/output security controls as specified in the NARA IT Security Handbook, Operations Controls.

Unauthorized individuals cannot read, copy, alter, or destroy information in printed form or on media removed from the information system. Media accountability and control mechanisms (e.g., audit trail logs) provide protection comparable to that for equivalent paper documents. Electronic media is controlled and protected in a manner similar to that used for paper materials. Output from the information system is given only to authorized users.

Appropriate security labels that reflect any distribution limitations and handling caveats of the information are affixed to all information system output, which includes printed output. Removable information storage media contains external labels indicating the distribution limitations and handling caveats of the information.

Only authorized users pick up, receive, or deliver input and output information and media from the information system. Appropriate controls are established for all information entering or leaving the facility, including for mailing media and/or printed output from the information system. Erroneous or unauthorized transfer of information, regardless of media or format, is precluded.

Information system hardware and machine-readable media is cleared, sanitized, or destroyed before being reused or released outside of the organization. Retired, damaged, discarded, or unneeded information is disposed in a manner that prevents unauthorized persons from using it. Information is never disclosed during disposal unless authorized by statute. Cleared or sanitized media that previously contained information at a designated FIPS Publication 199 security category (for confidentiality) is reused at the same or higher security category. Sanitized media is downgraded only with appropriate approval(s).
The media and output control is monitored and enforced by the system manager.

Destruction of Paper Media

Hard copy documents are destroyed when no longer needed. For information requiring such protection, destruction methods for organizational information in paper form are as follows:

(i) Burning – the material is burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle is separated to ensure all pages are consumed
(ii) Mulching or pulping – all material is reduced to particles one inch or smaller
(iii) Shredding or disintegrating - paper is shredded in cross-cut shredders (preferred) or strip shredders (alternative)

Information storage media is destroyed in accordance with organization-approved methods. An authorized contractor accomplishes document destruction in the absence of the organization's direct participation.

Release of Systems and Components

Equipment removal procedures for information systems and components that have processed or contained organizational information are followed. This includes inspection of the information system by designated individuals to ensure that all media, including internal disks, have been removed or sanitized.
Only approved equipment or software is used to degauss or overwrite magnetic media containing organizational information. Degaussing equipment is tested for correct performance annually. Each action or procedure taken to overwrite or degauss such media is verified.

Optical Disks

Optical disks (including compact disk/read only memory, write once/read many, digital versatile disk, and read-write compact discs) offer no mechanism for sanitization. Therefore they will be destroyed.

Sanitizing

Magnetic media containing organizational information are sanitized by use of an approved degaussing procedure.

Clearing

To clear magnetic media, all memory locations are overwritten three times (the first time

with a random character, the second time with a specified character, and the third time with the complement of that specified character). The success of the overwrite procedure is verified through random sampling of the overwritten media. Items that have been cleared (i.e., not sanitized) remain at the previously designated FIPS Publication 199 security category (for confidentiality) and remain in a secure, controlled environment.

NARA has standard rules of behavior, which all users must acknowledge during new user orientation and annual user training. In addition users (employee, contractor, intern, or others performing work for NARA with access to NARA IT resources) of NARA information technology and computing resources, are required to comply with NARA regulations, policies, procedures, and guidelines regarding the protection of NARA automated information systems from misuse, abuse, loss, or authorized access. Users understand that they will be held accountable for their actions related to the NARA data, information, and computing resources entrusted to them. Users further understand that they may be subject to criminal prosecution, and/or administrative disciplinary action, including reprimand, suspension from duty without pay, or removal from my position and/or Federal employment for failure to comply with the states rules of behavior. The complete rules of behavior are outlined in the System Security Plan for the DCU system.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

N/A

Section 4: Sharing of Collected Information

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

System administrators and users will have access to the system

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.).

Individuals requiring access to information must be screened (e.g., verification of background checks and investigations as well as security and non-disclosure agreements) prior to being granted access authorization in accordance with organizational personnel security policies. Privileged users (i.e., individuals who are authorized to bypass significant technical and operational controls), are screened prior to access and periodically every two years. For prospective employees, references are contacted and background checks performed, as appropriate. Periodic reinvestigations are performed no more than every five years, consistent with the criticality/sensitivity rating of the position, according to criteria from the Office of Personnel Management. Security agreements are

required for employees and contractors assigned to work with mission information. The period during which nondisclosure requirements remain in effect is identified.

Each user or process is authorized the most restrictive set of privileges or accesses needed for the performance of authorized tasks.

Information system owners identify authorized users and their respective access authorizations. Emergency and temporary access authorizations to the information system are explicitly approved by designated organization officials, monitored, and removed as soon as no longer required. Where appropriate, access is authorized based on time and/or location. Security administrators set parameters in security software to provide access as authorized and restrict access that has not been authorized. This includes access to files, load libraries, batch operational procedures, source code libraries, security files and operating system files.

Comprehensive account management, monitored and enforced by the system manager ensures that only authorized users can gain access to information systems. Account management includes:

- Identifying types of accounts (individual and group, conditions for group membership and associated privileges)
- Establishing an account (i.e., required identification, approval, and documentation procedures)
- Activating an account
- Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators)
- Terminating an account

When the user's employment is terminated, the organization terminates information system access, conducts exit interview, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures the individual no longer has access to official records created by the employee that are stored on organizational information systems.

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

Each user or process is authorized the most restrictive set of privileges or accesses needed for the performance of authorized tasks. Levels of access are outlined above.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access (please list processes and training materials)?

See number 2, above.

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 regulatory measures addressed?

No. Contractors performed the installation of the software components and were required to sign the on-site access documents for entering the building. There was not a contract except for the purchase contract for the software and installation. NH/ITSS performs the on-going maintenance of the Operating System software and hardware related to the system.

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared. If no, continue to question 8.

There is no data exchange between the NPRC Document Conversion Utility and other NARA systems.

However, once the paper records have been scanned, they are transmitted to the EHRI eOPF system. This is done via an external interface connection. It consists of a VPN session using the Connect: Direct Secure Plus software to the OPM owned EHRI eOPF system application. This external interface (OPM owned EHRI eOPF system application) is covered by its own system security plan which is in place.

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?

The external interface, the OPM owned EHRI eOPF system application, is covered by its own security plan and PIA. OPM is responsible for these certifications.

In addition there are two agreements that govern this system:
1. MOU between OPM and NPRC-CPR
2. Service Level Agreement (SLA)/MOU/ISA between OPM EHRI-eOPF system, NPRC-CPR and NBC

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

Individual data owners are responsible to manage and secure any personally identifiable information which resides in the COPR-OPM Document Conversion Project according to agency directive and existing MOU's between NARA and OPM. NARA's Senior Agency Official for Privacy is responsible for ensuring compliance with the privacy rights of the public and NARA employees.

9. Will other agencies share data or have access to the data in this system (Federal, State, Local, or Other)? If so list the agency and the official responsible for proper use of the data, and explain how the data will be used.

Yes, the data in the system will be shared with OPM. The CPR-OPM Document

Conversion Project will store and transmit electronic copies of civilian personnel files (OPFs). Civilian OPFs will be scanned into the system and these digitized files will be transferred to the OPM Electronic OPF system.

Section 5: Opportunities for Individuals to Decline Providing Information

1. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

N/A

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

N/A

Section 6: Security of Collected Information

1. How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures (e.g., data models, etc.).

The data in the system are scanned images of original paper OPFs. The OPFs transferred to NARA's physical custody are assumed to be accurate, timely and complete at the time of transfer from the originating agency. These records remain under the custody of the OPM and are subject to the provisions of the Privacy Act, which authorizes individuals to request the amendment of inaccurate information. Such requests, however, are adjudicated by OPM, not NARA.

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

N/A. The system used to convert the EHRI back file projects is currently maintained only at the NPRC/CPR Document Conversion Unit (DCU) in St. Louis, Missouri.

3. What are the retention periods of data in this system?

The retention period for the scanned OPF images is temporary. Once the images are transmitted to the EHRI-eOPF system, OPM conducts a 10% review of the images. This review takes 1-2 months. Upon completion of the OPM review, NPRC/CPR is given confirmation that the images are acceptable and the images housed within the Document Conversion Utility may be purged.

4. 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? Cite the disposition instructions for records that have an approved records disposition in accordance with, FILES 203. If the records are unscheduled that cannot be destroyed or purged until the schedule is approved.

After the scanned OPF images have been successfully transferred to the EHRI-eOPF system and OPM/employing agency has performed a quality review with acceptable results, the DCU System Administrator will purge the images from the directory on the server where the images reside. There is no recycle bin on the server in which the images can be retained once deleted. The DCU System Administrator at CPR has documented the procedures for purging the DCU system.

The "official record" copies of the OPF images are stored on OPM's EHRI-eOPF system. The images saved in the Document Conversion Utility are temporary working copies only.

The paper OPFs from which the scanned images have been made are not being destroyed at this time. OPM is working with Department of Justice and NARA to determine an appropriate retention period.

5. Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, describe.

No.

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

N/A

7. Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy? Yes

8. Has a risk assessment been performed for this system? If so, and risks were identified, what controls or procedures were enacted to safeguard the information? A risk assessment was performed on the DCU system 4/3/2007. The overall system risk was identified as Medium-Low. Temperature and humidity were identified as medium risks for the DCU servers. This risk has been mitigated through the integration of an additional air conditioning unit in the server room to augment facilities HVAC equipment.

The DCU system contains privacy data. System personnel know they are working with privacy data and treat it accordingly, but residual risk exists in this arena as human error and mistakes can inadvertently be made while handling this data..

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.
NARA conducts vulnerability scans on all network devices, including the DCU servers, on a monthly basis per a predefined schedule. A quarterly report of open vulnerabilities is compiled and analyzed. In addition, a subset of NIST 800-53 controls are tested for NARA systems on an annual basis.

10. Identify a point of contact for any additional questions from users regarding the security of the system.
Richard Morgan
National Digital Imaging Specialist
Email: Richard.morgan@nara.gov
Phone: 314.801.9274

Section 7: Is this a system of records covered by the Privacy Act?

1. Under which Privacy Act systems of records notice does the system operate? Provide number and name.
Records in this system are owned by the Office of Personnel Management. The Privacy Act system of records notices that apply to these records are published by the OPM.

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

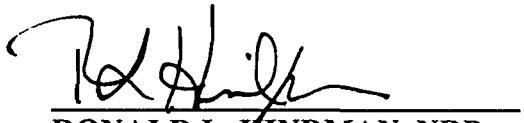
Any modifications to the Privacy Act system or records notices that may apply to records in this system are the responsibility of the OPM. There are no modifications to DCU system at this time.

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?
No

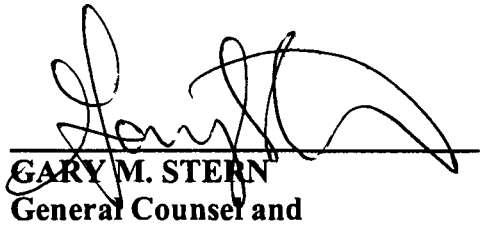
2. If so, what changes were made to the system/application to compensate?
N/A

The Following Officials Have Approved this PIA



(Signature) 9/5/08 (Date)

RONALD L. HINDMAN, NRP
Director, National Personnel Records Center (NPRC) and
NPRC Registry Files System Owner
Room 2075
Phone: 314.801.0574



(Signature) 9/9/08 (Date)

GARY M. STERN
General Counsel and
Senior Agency Official for Privacy (NGC)
Room 3100, AII
Phone: 301.837.3026

(Signature) 9/11/08 (Date)

MARTHA MORPHY
Assistant Archivist for Information Services and
Chief Information Officer (NH)
Room 4400, AII
Phone: 301.837.1992