U.S. Department of the Treasury
Financial Management Service (FMS)
Digital Check Imaging (DCI) Replacement
Privacy Impact Assessment Template

Name of Project: Digital Check Imaging (DCI) Replacement
Project's Unique ID: DCI

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- FMS IT Security Manager
- FMS AC-area Privacy Act Liaison

Also refer to the signature approval page at the end of this document.

For purposes of completing any FMS PIA, "data" means any information on an individual in identifiable form, i.e., any information that can be used to identify an individual.

A. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes

a. Is this information identifiable to the individual[1]?

Yes

b. Is the information about individual members of the public?

Yes

[1] "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

c. Is the information about employees?

Yes

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

DCI Replacement allows users to request, retrieve, view, and print all digitized U.S. Department of the Treasury (Treasury) checks that have been processed by the FRBs and have been captured and archived by the Federal Reserve System (FRS). The four Regiona l Financial Centers (RFCs) and the Birmingham Debt Management Center also use DCI Replacement to scan reclamation documentation in support of PACER On-Line (POL) claims and accounting processing. In addition, the system is used to match images with Claims Documentation.

FMS has a requirement to retrieve images of scanned reclamation documents for an indefinite period of time. Digital images of scanned reclamation documents, and digital check images must have a usable retrieval life of at least seven years with no degradation in image quality.

FMS and FRS jointly sponsor the DCI Replacement project, which captures and archives images of government checks. FMS issues, and services payments made by the Treasury and U.S. Government agencies. The FRS processes approximately 300 million checks per year on behalf of FMS.

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

The following legal authority authorizes the development of this system application:

- Chapter 4000 Section 15 of the Federal Reserve Act, adopted December 23, 1913, as amended (12 U.S.C. 391), and Section 10 of the Act of June 11, 1942, as amended (12 U.S.C. 265) authorizes the Secretary of the Treasury to set forth regulations to FRBs. In addition, Treasury is authorized by 31 CFR 240.3 to decline payment on any Treasury check bearing forged or unauthorized endorsements. Title X of the Competitive Equality Banking Act of 1987, Public Law No. 100 –86 authorizes Treasury to limit the payability and claimability of checks drawn on the Treasury
- Public Law 100-86, Competitive Equality Banking Act of 1987, Title X-Authorizes Treasury to limit the pay ability and claim ability of checks drawn on the Treasury

C. <u>DATA in the SYSTEM:</u>

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

The individuals covered by the system are payees/recipients of U.S. Government payments (e.g. Social Security Administration benefits, Internal Revenue Service tax refunds, Federal salaries, etc.)

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

Digitized check images from the FRS are the primary source of information in the DCI Replacement application. A secondary source of information is reclamation documentation used to support PACER On-Line (POL) claims and accounting processing.

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 source of the information is not directly from the individual. Federal Program Agencies (FPAs) provide the payment files to FMS. The payment files contain check information. The check information is directly related to the individual.

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

FMS, FRS and Federal Program Agencies (FPAs) that partner with FMS to disburse their payments provide the data used in the DCI Replacement system.

c. What State and 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?

Employee – None
Public – Digitized check images and supporting documentation

3) Accuracy, Timeliness, and Reliability

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

Payment data comes from FMS Regional Financial Centers (RFCs). Each RFC is responsible for the accuracy of the payment data submitted. FMS issues payments at the request of a Federal Program Agency (FPAs).

b. How will data be checked for completeness?

The DCI Replacement customer will verify that the digitized check image requested contains the correct name, amount, check symbol serial number, signature and various bank stamps on the back of the digitized check image. However, this only occurs when a claim has occurred with the check and FMS or a FPA is researching the claim.

c. Is the data current?

Yes. The DCI Replacement system has a requirement to store PACER documents for an indefinite period. The DCI Replacement system stores digitized check images for 60 days.

d. Are the data elements described in detail and documented?

No.

D. <u>ATTRIBUTES OF THE DATA:</u>

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

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

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

No

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

No

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

The DCI Replacement application does not create new data.

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

Data integrity/validation controls include virus protection, intrusion detection, the testing of existing security controls, and the monitoring of system performance. Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information has retained its quality and has not undergone unauthorized alteration. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements.

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

Controls are used for the marking, handling, processing, storage, and disposal of input and output information and media to protect the data and prevent unauthorized access when processes are being consolidated.

8) How will the data be retrieved?

Digital check images and supporting documentation are requested by an authorized user via PACER. The digital check images are ordered from the Federal Reserve System (FRS) through the DCI Replacement system. The digital check images are downloaded to the DCI Replacement database from the FRS.

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

No reports are produced on individuals.

10) 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 individuals can grant consent.)

None.

E. <u>MAINTENANCE AND ADMINISTRATIVE CONTROLS:</u>

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 DCI Replacement system is operated at one site.

2) What are the retention periods of data in this system?

Check images are purged after 60 days. The number of days can be increased or decreased at the discretion of FMS management. PACER has a legal requirement to retain scanned documents for an indefinite period of time.

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?

The oldest PACER documents were created in July, 2000. Currently, the retention period is indefinite; consequently, procedures have not been established to govern the disposition of PACER documents from the DCI Replacement database. DCI Replacement does not produce any reports.

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

No

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

N/A

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

No

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

None

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

N/A

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

.002 Payment Issue Records for Regular Recurring Benefit Payments
.010 Records of Accountable Officers' Authority with Treasury
.016 Payment Records for Other Than Regular Recurring Benefit Payments

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

N/A.

F. ACCESS TO DATA:

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

Table A: DCI Replacement – Access to the Data

Roles	Data Access
• Developers (contractors)	• Developers will **not** have access to production data • Developers will have access to test data • Developers will have access to development data
• Database Administrator (DBA)	• DBAs will have limited access to production data • DBAs will have unlimited access to test and development data.
• Application Administrator	• Resetting database print queues • Purge erroneous print jobs • Copying check images to CD-ROM
• DCI Replacement Internal User	• READ access only to DCI Replacement functions and tables
• DCI Replacement External User (FPAs)	• READ access only on DCI Replacement tables

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

A user with access to PACER On-Line (POL) will also have access to DCI Replacement. Criteria, procedures, controls and responsibilities regarding access are documented.

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

Users will access the DCI Replacement system through the PACER On-Line (POL) system. The user's access to DCI Replacement data will be restricted. A user will only be allowed to access digitized check images and supporting check documentation based on their Agency Location Code (ALC).

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

Yes. Controls are in place to prevent the misuse or unauthorized use of data by those having access. The DCI Replacement – Rules of Behavior is the primary source of information to identify the various controls in place.

Rules of Behavior establish a formal contract between the users of a system and the managing organization, stipulating acceptable use and security responsibilities. In accordance with NIST SP 800-18, *Guide for Developing Security Plans* for Information Technology Systems, a set of Rules of Behavior must be established in writing. The Rules of Behavior are made available to every user, (system administrators, developers, database administrators, etc.), requesting access to the system. These rules contain a signature page/block for acknowledging receipt by the users. The Rules of Behavior must clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules also state the consequences of inconsistent behavior or noncompliance.

FMS has established a baseline set of FMS Rules of Behavior that are included in the *FMS Information Technology Security Standards Manual*, February 17, 2005, Section 5. The DCI Replacement Rules of Behavior are contained in Appendix C of the DCI Replacement Security Plan. FMS requires the Rules of Behavior to be read and acknowledged before employees and contractors are granted access to the application.

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?**

Contractors are involved in the design and development of the DCI Replacement system. Contractors will be involved in the maintenance of the system. The Digital Imaging (DI) Statement of Work (SOW) specifies that the contractors must follow the FMS Systems Development Methodology (SDM) and other FMS Standards. The risk level of this contract has been determined to be "Moderate". Contractors need a security clearance. Contractors must be either US citizens or resident aliens and must wear identification badges while in FMS facilities.

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

No

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

The Financial Management Service (FMS); Regional Operations (RO), Financial Operations (FO), and Information Resources (IR) will be responsible for protecting the privacy rights of the public and employees affected by the interface.

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

Yes. Federal Program Agencies (FPAs) who disburse payments through FMS may have access to the DCI Replacement system.

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

DCI Replacement allows FPAs to request, retrieve, view, and print all digitized U.S. Department of the Treasury (Treasury) checks that have been processed by the FRBs and have been captured and archived by the Federal Reserve System (FRS). The four Regional Financial Centers (RFCs) and the Birmingham Debt Management Center also use DCI Replacement to scan reclamation documentation in support of PACER On-Line (POL) claims and accounting processing. In addition, the system is used to match images with Claims Documentation.

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

The Financial Management Service (FMS); Regional Operations (RO), Financial Operations (FO), Information Resources (IR); as well as, Federal Program Agencies (FPAs) will be responsible for assuring proper use of the data.