Central Application Tracking System (CATS)

Privacy Impact Assessment (PIA)

Version 1.0

April 28, 2013

Prepared by:

Office of the Comptroller of the Currency (OCC)

Security & Compliance Services (SCS)

Comptroller of the Currency
Administrator of National Banks

US Department of the Treasury

DOCUMENT CHANGE CONTROL

Version	Date	Summary of Changes	Pages Affected	Changes Made By:
1.0	April 28, 2013	Updated for ATO submission	All	SCS

NOTE

This document was prepared in support of the system's Security Assessment and Authorization effort. The document was developed in accordance with, or following the guidance contained in, the following:

- *The Privacy Act of 1974* (Public Law 92-132, 5 U.S. C. 552a).
- *Federal Information Security Management Act of 2002* (Title III of P.L. 107-347).
- Section 208 of the *E-Government Act of 2002* (Public Law 107-347, 44 U.S.C. Ch 36), April 17, 2003.
- Office of Management and Budget (OMB) Memorandum M-03-18, *Implementation Guidance for the E-Government Act of 2002*, August 1, 2003.
- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003.
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006.
- OMB Circular No. A-130**,** Revised, (Transmittal Memorandum No. 4)**:** *Management of Federal Information Resources*, 28 November 2000.
- Computer Matching and Privacy Act of 1988 (Public Law 100-503).
- Department of the Treasury Publication, TD P 25-05, *Privacy Impact Analysis Manual*, dated July 2006

Table of Contents

PRIVACY IMPACT ASSESSMENT

1. INTRODUCTION

PII is ―any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information[1].

To *distinguish* an individual is to identify an individual. Some examples of information that could identify an individual include, but are not limited to, name, passport number, social security number, or biometric data. In contrast, a list containing only credit scores without any additional information concerning the individuals to whom they relate does not provide sufficient information to distinguish a specific individual.[2]

The following list contains examples of information that may be considered PII. [3]

- Name, such as full name, maiden name, mother‘s maiden name, or alias
- Personal Identification Number, such as Social Security Number (SSN), passport number, driver‘s license number, taxpayer identification number, patient identification number, and financial account or credit card number
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or title number and related information
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

---

[1] GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008, http://www.gao.gov/new.items/d08536.pdf.

[2] Information elements that are not sufficient to identify an individual when considered separately might nevertheless render the individual identifiable when combined with additional information. For instance, if the list of credit scores were to be supplemented with information, such as age, address, and gender, it is probable that this additional information would render the individuals identifiable.

[3] NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

2. SYSTEM IDENTIFICATION

2.1 Name of System, Project, or Program:

Central Application Tracking System (CATS)

2.2 Responsible Organization

Chief Counsel's Office (CCO)
Office of the Comptroller of the Currency (OCC)
400 7th Street S.W.
Washington, DC 20024.

2.3 Information Contact(s)

Names of persons knowledgeable about the system, the system and data owner, security personnel, etc.:

See PTA (Privacy Threshold Analysis) document.

2.4 Security Categorization

The system was assessed in its Security Categorization Report (SCR) as MODERATE, under guidance contained in Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, as follows:

MISSION AREA	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Program Evaluation	Low	Low	Low
Program Monitoring	Low	Low	Low
Policy & Guidance Development	Low	Low	Low
Management Improvement	Low	Low	Low
User Fee Collection	Low	Low	Low
Customer Service	Low	Low	Low
Official Information Dissemination	Low	Low	Low
Public Affairs	Low	Low	Low

MISSION AREA	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Central Records & Statistics Management	Moderate	Moderate	Low
Personal Identity and Authentication Information	Moderate	Moderate	Moderate
Record Retention	Moderate	Moderate	Low
Information Management	Moderate	Moderate	Low
Financial Sector Oversight	Low	Low	Low
Industry Sector Income Stabilization	Low	Low	Low
Community & Regional Development	Low	Low	Low
Standards Setting/Reporting Guideline Development	Low	Low	Low
Permits & Licensing	Moderate	Moderate	Low

2.5 System Operational Status

CATS is in the Operational phase in accordance with the system operational status as outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 Revision 1. CATS deployed to production in April 2013.

The status of the system is: Operational – the system is in production.

2.6 General Description/Purpose

CATS is a replacement system for the Corporate Activities Information System (CAIS) and the e-Corp system. CATS will provide the Licensing and Community Affairs Departments within OCC the capability to electronically capture, effectively monitor, facilitate and report on the processing of filings submitted. CATS accepts information pertaining to 12 broad types of filings categories related to the corporate structure of national banks. The types of filings include bank charters, conversions, branch openings/closings/relocations, acquisitions, and subsidiary activities.

The OCC Licensing Department instructs and supports national banks in obtaining appropriate authorizations to conduct banking activities in accordance with Federal laws. The OCC Community Affairs Department conducts outreach and develops many publications to help national banks provide financial services to underserved markets.

2.7 System Environment

CATS will operate within the OCC enterprise network environment, offering external users the ability to access CATS functionality via the BankNet DMZ. CATS components will utilize Windows 2008 R2, Microsoft SQL 2008 Enterprise and Internet Information Services 7.0, with interconnectivity to the Operational Data Store. A Google Search Appliance component offers data search capability within the CATS data architecture. Users will access CATS using their OCC workstations (internal) or through the OCC VPN (external); BankNet accounts will be created for applicants at financial institutions.

2.8 Future Changes to CATS

CATS Release 1 deployed to production in April 2013. There are three releases planned for the OCC CATS deployment: Pilot, Release 1, and Release 2.

2.9 System Interconnection/Information Sharing

The CATS system will interconnect and share information using the internal OCC email system, the Institutional Database, the Operational Data Store, OCC's Document Management System, Records Management System, Examiner View (Supervision's database), CDID (Community Development Investment Database), PTS (Project Tracking System) and the DOJ/CAS system (electronic fingerprints).

3. PRIVACY IMPACT ASSESSMENT

3.1 Privacy Assessment

The following paragraphs detail the Privacy Assessment applicable to CATS.

3.1.1 Does this system collect any personal information in identifiable form about individuals?

Yes ☒ No ☐

3.1.2 Does the public have access to the system?

Yes ☒ No ☐

3.1.3 Has a PIA been completed in the past?

Yes ☒ No ☐

The CATS system has completed a SA&A, and a PIA was completed as a part of this process.

3.1.4 Has the existing PIA been reviewed within the last year?

Yes ☐ No ☐ N/A ☒

3.1.5 Have there been any changes to the system since the last PIA was performed?

Yes ☐ No ☐ N/A ☒

3.2 Data in the System/Application

3.2.1 What elements of PII are collected and maintained by the system?

- Name
- Date of birth
- Place of birth
- Social security number (SSN)
- Citizenship information
- Home and work address information
- Home and work telephone information
- Home and work e-mail information
- FBI criminal check data and accompanying adjudication data
- Background investigation data and accompanying adjudication data

3.2.2 Why is the information being collected?

CATS will be used to collect and/or maintain PII data contained in Interagency Biographical and Financial Reports (IBFR). IBFRs are required by FDIC statute for all directors, senior executives, and key management personnel of financial institutions examined by the OCC. PII data is authorized for collection by the OCC in accordance with the Privacy Act of 1974, 5 U.S.C 552a, as announced in Department of the Treasury Notice of Systems of Records, Federal Register, Volume 75, Number 172, September 7, 2010.

3.2.3 What are the sources of the information in the system?

Sources of information include directors, senior executives, and key management personnel of financial institutions; IBFR responses from other Federal agencies; and OCC bank examiners.

3.2.4 How will the data collected from sources other than Federal agency records or the individual be verified for accuracy?

Not applicable. Information entered into CATS by bank examiners is supplied by the individuals at financial institutions.

3.2.5 Who will have access to the data and how is access determined?

CATS will use role-based access control to control access to PII. Bank examiners will have access to records that they have entered, as well as to IBFRs for bank employees within the scope of individual examiner responsibility. CATS users will not be permitted to perform general PII searches against the entirety of the CATS data store.

3.2.6 Describe the administrative and technological controls that are in place or that are planned to secure the information being collected.

The CATS system architecture and data is protected by the Network Infrastructure (NI) GSS. The NI GSS provides primary security services and data security mechanisms in support of OCC systems and applications. These security services include identification and authentication (I&A), logical access controls, and auditing. The hosting facility is staffed at all times. Surveillance cameras are in place to monitor perimeter activity. All doors are alarmed and can only be opened with a valid and appropriate ID, security guard deactivation of locking mechanisms, or physical keys that are physically secured.

3.2.7 What opportunities will individuals have (if any) to decline to provide information or to consent to particular uses of the information?

Individuals will be presented with a privacy statement and will be offered an opportunity to decline to provide data.

3.2.8 What is the life expectancy of the data and how will it be disposed of when it is no longer needed?

PII data collected within CATS will be retained and disposed of in accordance with the OCC Record Control Schedule.

3.2.9 Is the system owned, operated, and maintained by a contractor?

Yes ☐ No ☒

3.3 System of Records (SOR) Notice

Does the collection of this information require a new system of records under the Privacy Act (5 U.S.C. § 552a) or an alteration to an existing system of records?

Yes ☐ No ☒

3.4 Security Assessment and Authorization

Has the system been assessed and authorized within the last three years?

Yes ☒ No ☐

Date ATO granted: April 29, 2013.

Note: The OCC Chief Counsel's Office determined that CATS is <u>not</u> a Privacy Act system.