Comptroller of the Currency
Administrator of National Banks
US Department of the Treasury

OCC

C-CURE

Privacy Impact Assessment (PIA)

January 2011

Version 1.3

Prepared by:

OM/ITS

Security and Compliance Services

DOCUMENT CHANGE CONTROL

VERSION	DATE	SUMMARY OF CHANGES	NAME
1.0	9/29/2008	Final draft	ISO
1.2	11/19/2008	Page 7, under section 2.4 SORN Impact Evaluation (correcting that C-CURE system **is** covered by an existing SORN).	ISO/K.Flores
1.3	1/13/11	Update/Review of Document	IRM/V.Curtis

Purpose

The Privacy Impact Assessment (PIA) is completed as a mandatory step in the certification and accreditation of IT systems, applications, and projects, that collect, process, store, and disseminate Personally Identifiable Information (PII). The PIA examines the ways in which PII data are managed and protected by the target of evaluation.

NOTE

This document was prepared in support of the system's Certification and Accreditation 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

Page

PRIVACY IMPACT ASSESSMENT

1. SYSTEM IDENTIFICATION

1.1 Name of System, Project, or Program:

C-Cure

1.2 Responsible Organization

Office of the Chief Financial Officer
Office of the Comptroller of the Currency (OCC)
250 E Street, Southwest Washington, DC 20219.

1.3 Information Contact(s)

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

See PTA (Privacy Threshold Analysis)

1.4 Security Categorization

The system was assessed in its Security Categorization Report (SCR) as, under guidance contained in Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003, as follows:

1.5 System Operational Status

The System is currently “Operational” because it is in the Operations & Maintenance Phase of the System Development Life Cycle (SDLC).

1.6 General Description/Purpose

Information Type	Confidentiality	Integrity	Availability
Corrective Action	Low	Low	Low
Program Evaluation	Low	Low	Low
Program Monitoring	Low	Low	Low
Policy and Guidance Development	Low	Low	Low
Management Improvement	Low	Low	Low
Official Information Dissemination	Low	Low	Low
Reporting and Information	Low	Moderate	Low
IT Security	Low	Moderate	Low
Business and Industry Development	Low	Low	Low
Financial Sector Oversight	Moderate	Low	Low
Judicial Hearings	Moderate	Low	Low
Legal Defense	Moderate	Moderate	Low
Legal Investigation	Moderate	Moderate	Moderate
Legal Prosecution/ Litigation	Low	Moderate	Low
Resolution Facilitation	Moderate	Low	Low
Inspections and Auditing	Moderate	Moderate	Low
Standards Setting/Reporting Guideline Development	Low	Low	Low
Overall Per Category	**Moderate**	**Moderate**	**Moderate**
System Overall	**Moderate**		

The OCC C-CURE system, categorized as a Minor Application, is a COTS product that is used to administer physical access authorizations for the Headquarters building, the Washington Learning Center, the Virginia Avenue Annex, the Data Center, and all of the District Offices.

C-CURE is used to perform ID card administration (coded picture badge) and to monitor card activity. The badges themselves contain a portion of the OCC’s official personnel credentials, i.e., the person’s photograph. Photos are generated using a digital camera that is considered to be an adjunct piece of equipment to the C-CURE system. Facility personnel must be successfully presented to a badge reader in order to gain access to the building(s) to which the user has authorized access. The application contains functionality that allows the system administrator to add, modify, and delete new facility doors and equipment; these are known as security objects. The application includes a visitor management module, which renders all daily visit badges inoperable at 6 PM. C-CURE is also used to monitor alarms (door contact, panic, glass break, motion detectors, and Heating, Ventilation, and Air Conditioning.

2. PRIVACY IMPACT ASSESSMENT

2.1 Privacy Assessment

The following paragraphs detail the Privacy Assessment applicable to C-Cure.

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

Yes ☒ No □

2.1.2 Does the public have access to the system?

Yes □ No ☒

2.1.3 Has a PIA been completed in the past?

Yes ☒ No □

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

Yes ☒ No □ N/A □

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

Yes □ No ☒ N/A □

2.2 Data in the System/Application

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

The information that the C-CURE system stores and creates badges from the following information: employee or contractor’s full name, color photograph of their face, categorization of position (employee, intern, or contractor), and an OCC badge number.

These personal identifiers are stored for staff only. For visitors to OCC, the CCURE system collects only first and last names.

2.2.2 Why is the information is being collected?

Employee and contractor information (names) are collected from individuals, when the individual requests for building pass, employee identification card and to assign privileges.

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

The sources of the information are collected from the Personal Identity Verification (PIV) Request form. This form must be completed prior to the issuance of an OCC badge. The form is completed by several personnel including the applicant, sponsor, registrar, and issuer.

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

Information collected on the PIV Request form is verified in accordance with HSPD-12 requirements.

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

Access to C-Cure is limited to Security and Compliance Services (SCS) office personnel, as determined by SCS management staff. ITS staff at the Landover Data Center also have limited access, for the purpose of server administration of the system.

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

All management, operational, and technical controls in place and planned for C-CURE are described in the System Security Plan, which must be approved in writing by various C-CURE management officials.

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

There is none.

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

We expect to retain the data until further notice.

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

Yes ☐ No ☒

2.3 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 ☐

Office of Management and Budget (MB) Circular A-130, *Management of Federal Information* Resources (Revised) (Transmittal Memorandum No. 4), December 2000, Appendix I, paragraph 4c (1) details which actions that may require a new or altered SORN.

2.4 Certification and Accreditation

Has the system been certified and accredited within the last three years?

Yes ☒ No ☐

Date ATO granted: **10/02/2008**