C-CURE

Privacy Impact Assessment (PIA)

Version 1.6

June 26, 2014

Prepared by:

Office of Comptroller of Currency (OCC)
Security & Compliance Services (SCS)
Division

DOCUMENT CHANGE CONTROL

Version	Date	Summary of Changes	Pages Affected	Changes Made By:
1.0	9/29/2008	Final draft	All	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).	7	ISO/K. Flores
1.3	1/13/2011	Update/Review of Document	All	IRM/V. Curtis
1.4	5/29/2012	Update during re-certification	All	SCS: COACT, Inc.
1.5	9/5/2012	Update/Review of Document	All	SCS: V. Curtis
1.6	6/26/2014	Update/Review of Document	6	Rodney Taylor

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.

Data and information types can be found in the applicable Security Categorization Report for the system.

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. 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:

C-CURE

2.2 Responsible Organization

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

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*, December 2003, as follows:

Table 1-1: High Water Marks for Information Types

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		

2.5 System Operational Status

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

2.6 General Description/Purpose

The OCC C-CURE system is a COTS product that is used to administer physical access authorizations for all OCC office locations. C-CURE is categorized as a Minor Application. The primary server is housed in the Ashburn, VA Data Center, and the backup server is housed in the OCC district office located in Dallas, TX. Workstations running C-CURE client software connect to the server to perform tasks, such as to program cards or monitor activity.

The C-CURE 9000 product is developed by Software House. The Office of Security (OS) engages contractor support to provide all the necessary support for the client software, server software, and related hardware. Contractor support must be physically present at the site to provide assistance, no remote connection is allowed.

Users of C-CURE verify their access to physical locations through the use of coded badges. The badges are programmed at Headquarters and all District Offices. Badges are printed with the user's name, photograph, and dates of expiration. Photographs are retrieved from a digital camera, which is considered an adjunct piece of equipment in the C-CURE information system. To verify their access to physical locations, users must present their badge to an appropriate reader. C-CURE is also used to monitor alarms (door contact, panic devices, and, motion detectors).

2.7 System Environment

The C-CURE system is made up of 3 components:

1. Servers. Servers contain a central database of security objects and authorizations. Clients connect to the server and view or make modifications to this database.

Once modifications are made, the C-CURE server sends these updates via TCP/IP to the panels or terminal servers. In addition to a central server, there can be multiple backup servers. While not in use, these servers connect to the main server and mirror its database. If there is a problem communicating to the central server, clients can be redirected to connect to the backup server.

2. Clients. C-CURE client software runs in Windows 7 workstations. Client software has much different functionality, which are described.

3. Security Objects. Security objects are panels that read information from badges and provide access to different areas of buildings. Security objects such as the IStar control panels are IP aware. ,.

4. According to RFC number ECCSp00029150, the C-CURE 9000 upgrade from version 2.01 to version 2.20, which was recently implemented on April 2014, is required to prove the implementation of an interface from the Personnel Administration and Security System (PASS). One of the objectives of PASS is to automate the entry of SmartID data into the C-CURE system. Automating the entry of SmartID data through a new interface is essential to maintaining a controlled set of SmartID data in C-CURE..

2.8 Future Changes to C-CURE.

2.9 System Interconnection/Information Sharing

The C-CURE system will have an interconnection with the Personnel Administration and Security System (PASS). The installation of C-CURE 9000 allows for the automation of SmartID data entry into the C-CURE system through PASS. The new interface with PASS is confirmed through the installation of C-CURE 9000. The C*CURE 9000 server will be polling a Lightweight Directory Services (LDS) instance that has been installed on the PASS presentation server.

3. PRIVACY IMPACT ASSESSMENT

3.1 Privacy Assessment

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

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 ☐

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 ☐ C-Cure was upgraded in May 2012.

3.2 Data in the System/Application

3.2.1 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.

3.2.2 Why is the information 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.

3.2.3 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.

3.2.4 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.

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

Access to C-Cure is limited to Office of Security (OS) office personnel, as determined by OS management staff. ITS staff at the also have limited access, for the purpose of server administration of the system.

3.2.6 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.

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

There are none.

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

The data is expected to be retained until further notice.

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 ☐

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 System of Records Report.

3.4 Certification and Accreditation

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

Yes X☐ No ☐

Date ATO granted: 09/29/11