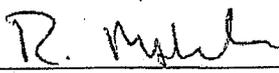


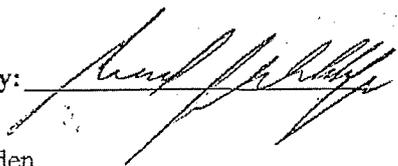
REVIEW AND APPROVAL SIGNATURES

The C-CURE Privacy Impact Assessment was prepared for the exclusive use in support of the Certification and Accreditation Program. The plan has been reviewed and approved at the responsible office, the Information Systems Security Officer, the Chief Information Officer, and at the Privacy Advocate level.

Reviewed by:  Date: 10/14/08
Rodney Taylor
Information System Security Officer (ISSO), C-CURE

Reviewed by:  Date: 10/10/08
Dave Woodson
Information Security Office

Reviewed by:  Date: 10/13/08
Roger Mahach
Chief Information Security Officer / Chief Privacy Officer

Approved by:  Date: 10/14/08
Ronald Shelden
Assistant Director, Critical Infrastructure Protection and Security

1 SYSTEM IDENTIFICATION

1.1 System Name/Title

The official system name is: C-CURE

1.2 Responsible Organization

Office of the Comptroller of the Currency
 Critical Infrastructure Protection and Security (CIPS)
 Office of the Chief Information Officer (OCIO)
 250 E Street, SW
 Washington, DC 20219-0001

1.3 Washington, DC 20219-0001 Information Contact(s)

See Table 1-1 – 1.3, Contact Information for C-CURE. Name of person(s) knowledgeable about, or the owner of, the system:

Table 1-1: System Owner Contact Information for C-CURE

System Owner / Information System Security Officer	
Name:	Rodney Taylor
Title:	Physical Security Specialist
Address:	Critical Infrastructure Protection and Security 250 E Street, SW Washington, DC 20219-0001
Phone:	(202) 874-3402
E-mail:	Rodney.Taylor@occ.treas.gov

Table 1-2: Privacy Officer Contact Information for C-CURE

Privacy Officer	
Name:	Roger Mahach
Title:	Chief Information Security Officer / Chief Privacy Officer
Address:	250 E Street, SW Washington, DC 20219-0001
Phone:	202-874-1023
E-mail:	Roger.Mahach@occ.treas.gov

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?

Y N

2.1.2 Does the public have access to the system?

No, C-CURE is not a publicly accessible system.

2.1.3 Has a PIA been done before?

Y N

This is the initial PIA for the C-CURE system.

Date first developed: May 2004

Date last updated: August 14, 2004

2.1.4 Has it been at least three years since the last PIA was performed?

Y N Has a Privacy Impact Assessment been completed?

2.1.5 Has the system changed since the last PIA was performed?

Y N

C-CURE was previously identified as a component of the major application formally known as the *Employee Security Major Application*. That system ceased to exist after OCC's revision of its FISMA System inventory in May 2007. C-CURE now stands alone as its own minor application in the current OCC FISMA System Inventory, and therefore must now have its own privacy threshold analysis.

2.2 Data in the System/Application

2.2.1 Describe the information to be collected, why the information is being collected, the intended use of the information, and with whom the information will be shared.

The information that the C-CURE system stores and creates badges from contains 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 C-CURE system collects only first and last names.

2.2.2 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.

2.2.3 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.

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

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

2.2.5 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.

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

Individuals have the ability to decline providing privacy information at the system entry points which are the institutions. These entry points have the responsibility to provide the individual with the opportunity to decline providing information. No other opportunities are provided by C-CURE for declining.

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

The current life expectancy of the data is currently the life of the system. Once the size reaches a point where disposition must be addressed, then C-CURE will dispose of information IAW federal regulations for financial information.

2.3 System of Records Notice (SORN)

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?

Y N

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 SORN Impact Evaluation

The C-CURE system is covered by one or more of the following SORNs, as published in the Federal Register / Vol. 70, No. 131 / Monday, July 11, 2005 / Notices. This notice covers all systems of records adopted by the OCC up to June 21, 2005. It includes:

- CC .100—Enforcement Action Report System
- CC .110—Reports of Suspicious Activities
- CC .120—Bank Fraud Information System
- CC .200—Chain Banking Organizations System
- CC .210—Bank Securities Dealers System
- CC .220—Section 914 Tracking System
- CC .340—Access Control System
- CC .500—Chief Counsel's Management Information System
- CC .510—Litigation Information System
- CC .600—Consumer Complaint and Inquiry Information System
- CC .700—Correspondence Tracking System

The following *SORN Impact Evaluation Summary*, details the evaluation of the stated criteria in order to determine if a new or altered SORN is required in support of the

OCC's C-CURE Minor Application. Any criteria marked with an "x" in the "Yes" column would indicate the likelihood of a new or altered SORN Report being required.

Table 2-1: SORN Impact Evaluation Summary

SORN Impact Evaluation Summary OCC C-CURE Application		
Criteria (OMB Circular A-130, Appendix I, paragraph 4c(1))	Evaluation	
	Yes*	No
1. A significant increase in the number, type, or category of individuals about whom records are maintained.		x
2. A change that expands the type or categories of information maintained.		x
3. A change that alters the purpose for which the information is used.		x
4. A change to equipment configurations (either hardware or software) that creates substantially greater access to the records in the system of records.		x
* Note: All "Yes" answers must be supported in detail		