

**U.S. Department of the Treasury
Office of the Comptroller of the Currency**

***Privacy Impact Assessment
CAG Remedy***

*Version 1.0
June 30, 2007*

Office of the Comptroller of the Currency
Department of the Treasury
250 E St. SW
Washington, DC 20219-0001

Controlled By: Chief Information Security Officer
Controlling Office: IT Security Office
Control Date: June 30, 2007
Decontrol On: Indefinitely


******* OCC Sensitive Security Information*******

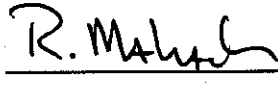
The information contained herein was produced, in whole or in part, by the Department of the Treasury, Office of the Comptroller of the Currency (OCC) for the benefit of the Department of the Treasury, OCC. As such, this information is the sole, proprietary, and exclusive property of OCC. Therefore, this information may only be used by (1) OCC, without limitation, (2) employees and agents whose access is necessary, and limited to, the accomplishment of the project tasks, and (3) any other individual or agency granted access by OCC under separate authority. All information contained herein is OCC Sensitive Security Information whether such information is in written, graphic, electronic, or physical form. Those granted access to the information by clause (2) or (3) above will hold these materials and information in strict confidence. Access and use of this information by any other entity or individual are strictly prohibited. Should you have any questions about the proper use or access to this information contained herein, please contact OCC's Chief Information Security Officer, Roger Mahach, at (202) 874-7276 for instructions.


CAG Remedy Privacy Impact Assessment Record of Changes				
Version No.	Date Released	Description of Change	Pages Affected	Changes Made By
1.0	June 30, 2007	Initial publication.	All	IT Security Office

REVIEW AND APPROVAL SIGNATURES

The CAG Remedy 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: 10/5/07
Dave Woodson
Information System Security Officer (ISSO)

Reviewed by:  Date: 10/9/07
Roger Mahach
Chief Information Security Officer

Reviewed by:  Date: 10/11/07
Gayle Rucker
Chief Privacy Officer

Approved by:  Date: 2 October 2007
Craig Stone
Deputy Ombudsman for Customer Assistance


Approved by:  Date: 10/5/07
Jackie Fletcher
Chief Information Officer

TABLE OF CONTENTS

1	SYSTEM IDENTIFICATION.....	1
1.1	System Name/Title.....	1
1.2	Responsible Organization.....	1
1.3	Information Contact(s).....	1
1.4	Security Categorization.....	2
1.5	System Operational Status.....	2
1.6	General Description/Purpose.....	2
1.6.1	Production Platform.....	7
1.6.2	Software.....	7
1.7	System Environment.....	8
1.8	System Interconnection/Information Sharing.....	8
2	PRIVACY IMPACT ASSESSMENT	9
2.1	Privacy Assessment.....	9
2.2	Data in the System/Application.....	9
2.3	System of Records Notice (SORN).....	11
2.4	SORN Impact Evaluation.....	12

LIST OF FIGURES

Figure 1-1: CAG Remedy Inputs.....	4
Figure 1-2: CAG Remedy Processing and Outputs.....	5

LIST OF TABLES

Table 1-1: System Owner Contact Information for CAG Remedy.....	1
Table 1-2: Privacy Officer Contact Information for CAG Remedy.....	1
Table 1-3: Information System Security Officer (ISSO) Contact Information for CAG Remedy.....	2
Table 1-4: Security Categorization Summary.....	2
Table 2-1: SORN Impact Evaluation Summary.....	13

1 SYSTEM IDENTIFICATION

1.1 System Name/Title

The official system name is: CAG Remedy. The Commercial Off-the-Shelf (COTS) product name is Remedy Action Request Version 6.01 patch 1351.

1.2 Responsible Organization

Office of the Chief Information Officer (OCIO)
Office of the Comptroller of the Currency (OCC)
250 E Street, Southwest
Washington, DC 20219-0001

1.3 Information Contact(s)

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

Table 1-1: System Owner Contact Information for CAG Remedy

System Owner	
Name:	Craig Stone
Title:	Director, Customer Assistance Group
Address:	Office of the Ombudsman Fulbright Tower Houston, TX
Phone:	(713) 336-4350
E-mail:	craig.stone@occ.treas.gov

Table 1-2: Privacy Officer Contact Information for CAG Remedy

Privacy Officer	
Name:	Gayle Rucker
Title:	Chief Privacy Officer
Address:	250 E Street, SW Washington, DC 20219-0001
Phone:	202-874-1023
E-mail:	gayle.rucker@occ.treas.gov

Table 1-3: Information System Security Officer (ISSO) Contact Information for CAG Remedy

Information System Security Officer (ISSO)	
Name:	Melinda Goodnight
Title:	CAG Remedy ISSO
Address:	Office of the Ombudsman Fulbright Tower Houston, TX
Phone:	(713) 336-4350
E-mail:	melinda.goodnight@occ.treas.gov

1.4 Security Categorization

The System is assessed for Security Categorization under the 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 1-4: Security Categorization Summary

SECURITY CATEGORIZATION SUMMARY			
Components	Impact Assessment		
	Confidentiality	Integrity	Availability
Services Delivery Support Information	Moderate	Moderate	Moderate
Rationale and Factors for Government Resource Management Information	Low	Moderate	Low
Economic Development Mission Area	Moderate	Low	Low
Litigation and Judicial Activities Mission Area	Moderate	Moderate	Moderate
Knowledge Creation and Management Mission Area	Low	Low	Low
High Water Mark	Moderate	Moderate	Moderate
CATEGORIZATION	Moderate		

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

The Customer Assistance Group (CAG) assists consumers who have questions or complaints about national banks and their operating subsidiaries. CAG provides service to three constituent groups:

- Customers of national banks and their subsidiaries – by providing a venue to resolve complaints.

- OCC bank supervision – by alerting supervisory staff of emerging problems that may potentially result in the development of policy guidance or enforcement action.
- National bank management – by providing a comprehensive analysis of complaint volumes and trend.

The CAG Remedy application is used by CAG Specialists, Tier One Customer Service Representatives, and the E-Business unit within the OCC.

The CAG Remedy application is used to:

- store information related to Consumer complaints involving financial institutions and provide access to documents related to consumer complaints
- store institutional data
- apply workflow rules to ensure prompt handling of Consumer complaints
- provide the data used for reporting purposes
- provide the data used by Banks to resolve Consumer complaints
- archive information related to cases
- receive Congressional data imports

The following diagrams outline the Input, Processing, and Outputs for the CAG Remedy Application:

**OCC Sensitive Security Information
CAG Remedy Privacy Impact Assessment
Version 1.0**

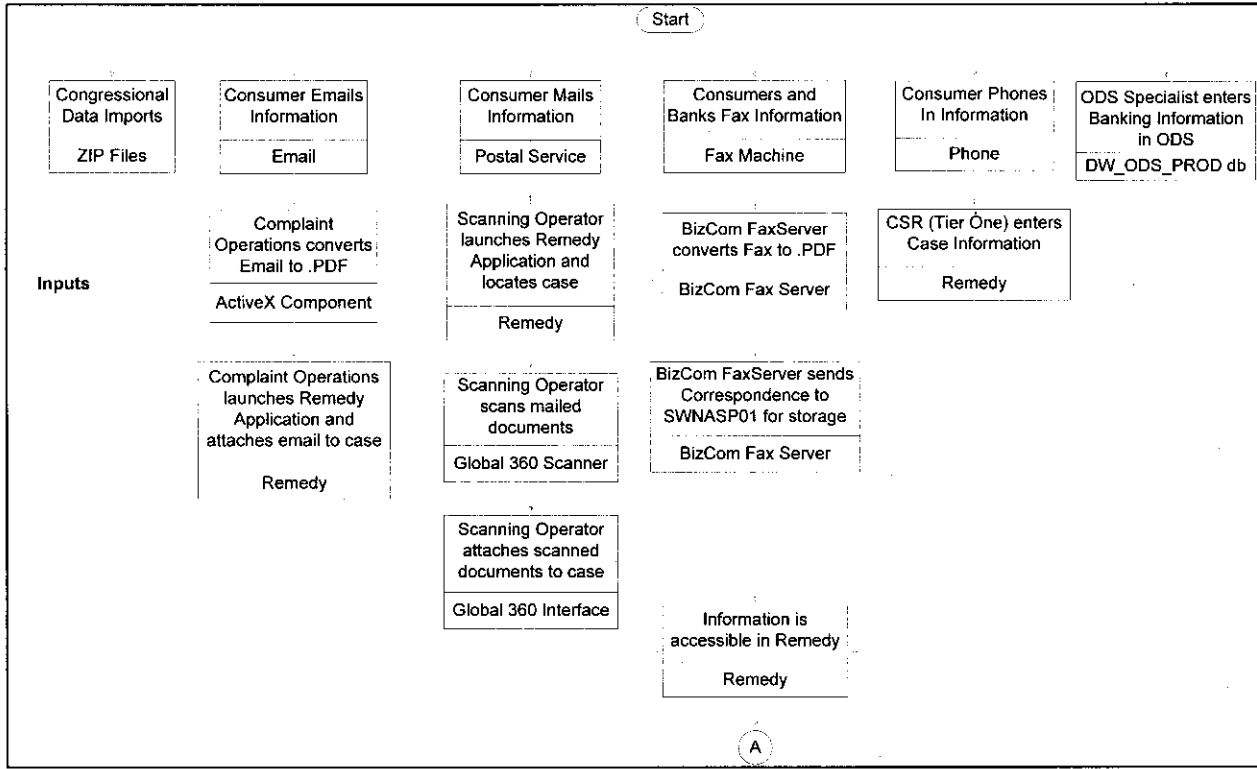


Figure 1-1: CAG Remedy Inputs

SECTION 1.6 TECHNICAL DETAILS ARE AVAILABLE AND ON FILE

Figure 1-2: CAG Remedy Processing and Outputs

Inputs to the CAG Remedy Application include Case Status Information, Customer Information, Case Detail Information, Case Assignment Information, and Documentation (Internal Communications sent from the OCC to the Consumer, External Communications sent from the Consumer, Consumer Representative or the Bank to the OCC). Documentation attached to complaint cases can be in the form of E-mail communications, mailed correspondence, faxed information, and information exchanged via phone conversations between the consumer and the CSR or Specialist.

Case Status Information – Case status information is entered in the Remedy system manually by the Specialists or automatically by the AR_Escalation and arprocess internal users. As the case progresses (or time passes) the Specialist or the Remedy Internal Users change the status of the case to indicate the next step in the process.

Customer Information – This information is entered in the system by the Specialist or Tier One CSR when the case is created.

Case Detail Information – The Consumer contacts the OCC and provides information related to the case. The Specialists or Tier One CSR enter detailed information related to the case based on information provided by the Consumer.

Case Assignment Information – When a case is entered in the system the case is assigned to a Specialist to indicate the individual responsible for reviewing the case.

Email Communications – The Consumer contacts the Complaint Operations Business Unit via email. The Complaint Operations Business Unit converts the email to .PDF format using the Adobe .PDF Conversion process. When the email is converted to .PDF format, the Complaint Operations Business Unit launches the Remedy Application, locates the case to which the documents apply, and attaches the emails to the respective case.

Mailed Correspondence – Consumers and Banks mail information to the Comptroller’s Office. When the Scan Operators receive the information, they launch the Remedy application and search for the case to which the documents belong. The document(s) are placed on the Global 360 ScanCom scanner, scanned, and automatically attached to the respective case. Scanned documents are actually stored on the SWNASP01 file server, but are accessible via the Remedy application.

Faxed Correspondence – Consumers and Banks fax information to the OCC. When the fax is received, the BizCom Faxserver queues the incoming faxes, converts the fax to .PDF format, and stores the documents on the SWNASP01 file server. The .PDF files are accessible via the Remedy application, but stored on the file server.

Phone Communications – Consumers contact the OCC via phone with inquiries or information related to consumer complaints. The Tier One CSR enters information in the Remedy application (SWSQLPARS00) related to the Consumers case. As the status of the case progresses, the consumer continues to follow-up and the Tier One CSR or Specialist updates the case detail.

Institutional Data – Institutional data (Bank Information) is stored on the DW_ODS_PROD server. This information is entered in the Remedy application via DTS feed.

Outputs from the CAG Remedy Application include:

CAGNet Reporting –The CAGNet application (outside the scope of this C&A) is used by Banks to display information related to Consumer complaints. This application is accessible via the BankNet website. When changes occur in Remedy the MS Replication process runs stored procedures to transfer data from the SWSQLPARS00 Remedy application server to the SQL Server for CAGNet Data. Data for CAGNet banks is transferred via the CAGNet transfer process every 5 minutes. The CAGNet functionality displays information related to the Complaint application.

NextGen Reporting – The NextGen application is used by CAG Personnel to generate reports on data stored in the complaint database (CAGReports). The NextGen application is accessible via the OCC website. When changes occur in Remedy the MS Replication process runs stored procedures to transfer data from the Remedy SWSQLPARS00 application server to the CAGReports database currently located on the HQSQLV106P SQL server.

Emails via MAPI – Based on rules within the Remedy system, workflow automatically sends emails to Specialists informing them of case information and/or reminders to follow-up on outstanding case related issues.

Remedy Data Queries – The Remedy application allows the Specialists to generate queries and perform advance searches on information stored in the Complaints applications.

Processing within the CAG Remedy Application includes:

- MS Replication runs stored procedures to select data from the Remedy application.
- MS Replication transfers data to CAGReports database.
- The DBA creates a view of the CAGReport database in the CAGNet database.
- Data is accessible by Specialist and Banks via NextGen application and CAGNet application.

Bankers review and return the case to the CAG; Server Timer checks every 5 minutes for changes; AR_Escalation process changes case status in Remedy.

SECTION 1.6 TECHNICAL DETAILS ARE AVAILABLE AND ON FILE

1.7 System Environment

Ombudsman TAC, maintains the servers. Ombudsman TAC also maintains user access to the application. The Ombudsman Office (the office) is located on the 34th floor of the 56 story Fulbright Tower in central Houston. The office shares the floor with the Houston Field Office. The lobby to the building is on the second floor. A guard desk is located by the entrance to the bank of elevators and the guard monitors numerous security cameras which cover each entrance to the building and the loading dock. All entrances to the office suite on the 34th floor are controlled by SIPS card readers connected to OCC HQ. An additional level of security is provided by a contract guard who sits in the reception area to the office suite. There is no intrusion detection system for the office.

Once in the office, it is possible to move between the Ombudsman space and the Field Office space without exiting the suite. The office consists of interior and exterior offices around the central core of the building. In the middle of the office is the central file room, LAN room, and computer storage closet. The LAN room is locked with a mechanical lock/key. Only the ITS representative and the Office Manager have keys. There was no fire extinguisher in the LAN room. The room was temperature controlled and very orderly. The servers were racked in cages, but the doors were removed. Backup tapes were locked in a different room. All personnel entering OCC facilities are required to wear an OCC-issued official badge.

1.8 System Interconnection/Information Sharing

Bank profile information is extracted from ODS by SQL DTS routines maintained by the DBA. Bank data is transferred weekly from ODS to Remedy AR server and Remedy Application server extracts data from Remedy AR server. Remedy forms populate information from CAG Remedy and AR CAG server bank information tables. The data is primarily used for decision support and to track and document the complaint process.

2 PRIVACY IMPACT ASSESSMENT

2.1 Privacy Assessment

The following paragraphs detail the Privacy Assessment applicable to the CAG Remedy.

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, CAG Remedy is not a publicly accessible system.

2.1.3 Has a PIA been done before?

Y N

This is the initial PIA for the CAG Remedy system.

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?

Not Applicable. This is the initial PIA for the CAG Remedy system.

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

Y N

Not Applicable. This is the initial PIA for the CAG Remedy system.

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 CAG Remedy system contains all data and information related to Case Status Information, Customer Information, Case Detail Information, Case Assignment Information, and Documentation (Internal Communications sent from the OCC to the Consumer, External Communications sent from the Consumer, Consumer Representative

or the Bank to the OCC). Documentation attached to complaint cases can be in the form of E-mail communications, mailed correspondence, faxed information, and information exchanged via phone conversations between the consumer and the CSR or Specialist.

There is information collected related to the consumer complaints involving financial institutions. This could include the bank name, the consumer's account number, the type of account, and the details of the complaint. If the consumer has an attorney or other representative, it could also contain information about that representative (e.g. name, title, phone number, etc.).

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

Inputs to the CAG Remedy Application include Case Status Information, Customer Information, Case Detail Information, Case Assignment Information, and Documentation (Internal Communications sent from the OCC to the Consumer, External Communications sent from the Consumer, Consumer Representative or the Bank to the OCC). Documentation attached to complaint cases can be in the form of E-mail communications, mailed correspondence, faxed information, and information exchanged via phone conversations between the consumer and the CSR or Specialist.

Bank profile information is extracted from ODS by SQL DTS routines maintained by the DBA. Bank data is transferred weekly from ODS to Remedy AR server and Remedy Application server extracts data from Remedy AR server. Remedy forms populate information from Remedy CAG and AR CAG server bank information tables.

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

For emailed communications, the Complaint Operations Business Unit converts the email to .PDF format using the Adobe .PDF Conversion process. For mailed correspondence, the document(s) are placed on the Global 360 ScanCom scanner, scanned, and automatically attached to the respective case. When a fax is received, the BizCom Faxserver queues the incoming fax, converts the fax to .PDF format, and stores the documents on the file server. Phone Communications are handled by the Tier One CSR who enters information in the Remedy application related to the consumer's case. As the status of the case progresses, the consumer continues to follow-up and the Tier One CSR or Specialist updates the case detail. This follow-up process includes verification of the consumer information. Many of the forms used by the Tier One CSR have drop-down boxes for those fields that are not narrative in content.

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

CAG Managers are the authorizing authority and the OMBD TAC technically provides that access. The OMBD TAC is responsible for access to the Remedy AR Server. The

system administrator will request access for a user to OMBD TAC by email indicating the person's name and application to access. OMBD TAC will determine if there is a need to purchase another site license and start the process to purchase if needed. OMBD TAC processes the request and notifies system administrator when access is granted. The system administrator will notify the user and assure the user has access to the system. Once the system is accessed, the main CAG login screen will appear displaying four fields. Username and password are the first two fields and must be provided in order to successfully login. The other two fields are Preference Server and Authentication.

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 CAG Remedy are described in the System Security Plan, which must be approved in writing by various CAG Remedy 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 CAG Remedy 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 CAG Remedy 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 CAG Remedy system is not 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 CAG Remedy Major 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 CAG Remedy Major 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		