

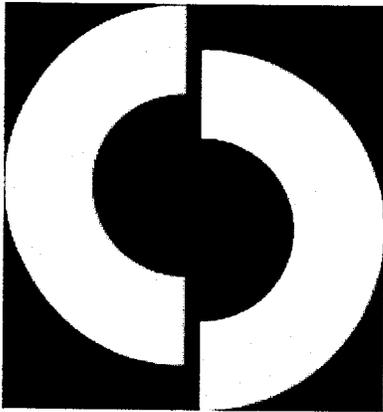
**OCC SENSITIVE
SECURITY
INFORMATION**

Office of the Comptroller of the Currency
**SENSITIVE SECURITY
INFORMATION
COVER SHEET**

**OCC SENSITIVE
SECURITY
INFORMATION**

**This Cover Sheet Is Not Controlled When
Separated From Attached Document(s).**

✓ PIA - GSS
File



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

*Privacy Impact Assessment
Network Infrastructure
General Support System (GSS)*

*Version 2.2
March 20, 2007*

Prepared by:

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

Controlled By: Jackie Fletcher

Controlling Office: Chief Information Officer

Accreditation Date: March 31, 2007

Re-Accreditation Date: March 31, 2010

WARNING

This document belongs to the Department of the Treasury, Office of the Comptroller of the Currency (OCC), Office of the Chief Information Officer (OCIO), Information Technology Network Infrastructure General Support System (GSS). It may not be released without the express permission of the OCIO. Refer requests and inquiries for the document to Dave Smith, Information System Security Officer (ISSO), at (301)324-3233 or at Dave.Smith@occ.treas.gov. (re: TD P 15-71, Chapter III, Section 23)

NOTE

This document was prepared in support of System Certification and Accreditation following the guidance contained in:

- *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.
- Office of Management and Budget (OMB) Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003.
- Office of Management and Budget (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

Record of Changes				
Version Number	Date Released	Description of Changes	Pages Affected	Changes Made By
1.0	02/14/2007	Initial Working Draft	All	SAIC
2.0	03/05/2007	Second draft – FISMA System Privacy Threshold Analysis Determination Checklist section 2.1 added	All	SAIC
2.1	03/06/2007	Correction of minor errata	All	SAIC
2.2	03/20/2007	Incorporated comments and suggestions Updated SORN section	All	SAIC

REVIEW AND APPROVAL SIGNATURES

The 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 Manager, and the Chief Information Officer and Privacy Advocate level.

Reviewed by: David A. Smith Date: 4-17-07
David Smith

Information System Security Officer (ISSO)

Reviewed by R. Mahach Date: 4-16-07
Roger Mahach

Chief Information Security Officer

Reviewed by Jim Devlin Date: 4-25-07
Jim Devlin

Chief Privacy Officer

Approved by: Richard Gordon Date: 4/16/07
Richard Gordon

Deputy Chief Information Officer

Approved by: Jackie Fletcher Date: 4/14/07
Jackie Fletcher

Chief Information Officer

Table of Contents

	<u>Page</u>
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
1.7 SYSTEM ENVIRONMENT	2
1.8 SYSTEM INTERCONNECTION/INFORMATION SHARING.....	2
2. PRIVACY IMPACT ASSESSMENT	4
2.1 FISMA SYSTEM PRIVACY THRESHOLD ANALYSIS DETERMINATION CHECKLIST	4
2.2 PRIVACY ASSESSMENT.....	5
2.3 DATA IN THE SYSTEM/APPLICATION	6
2.4 SYSTEM OF RECORDS (SOR) NOTICE.....	8
2.5 SOR IMPACT EVALUATION	9

**Office of the Comptroller of the Currency (OCC)
Network Infrastructure (NI) General Support System (GSS)
PRIVACY IMPACT ASSESSMENT**

1. SYSTEM IDENTIFICATION

1.1 System Name/Title

Network Infrastructure (NI) General Support System (GSS)

1.2 Responsible Organization

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

1.3 Information Contact(s)

Name of person(s) knowledgeable about, or the owner of, the system:

System Owner	
Name:	Jackie Fletcher
Title:	Chief Information Officer
Address:	250 E Street, SW Washington, DC 20219-0001
Phone:	202-874-4480
Email:	Jackie.fletcher@occ.treas.gov

Privacy Officer	
Name:	Jim Devlin
Title:	Chief Privacy Officer
Address:	250 E Street, SW Washington, DC 20219-0001
Phone:	202-874-5013
Email:	Jim.devlin@occ.treas.gov

Information Systems Security Officer (ISSO)	
Name:	Dave Smith
Title:	NI GSS ISSO
Address:	250 E Street, SW Washington, DC 20219-0001
Phone:	301-324-3233
Email:	Dave.smith@occ.treas.gov

1.4 Security Categorization

The System is assessed for Security Categorization (SC) 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:

SECURITY CATEGORIZATION SUMMARY			
Components	Impact Assessment		
	Confidentiality	Integrity	Availability
Network Infrastructure	Moderate	Moderate	Moderate
Applications	Moderate	Moderate	Moderate
Data	Moderate	Moderate	Moderate
High Water Mark	Moderate	Moderate	Moderate
CATEGORIZATION	MOPDERATE		

1.5 System Operational Status

The System is currently **Operational**, in the Operations & Maintenance (O&M) Phase of the System Development Life Cycle (SDLC).

1.6 General Description/Purpose

The OCC Network Infrastructure (NI) is a General Support System (GSS) that provides core and critical information technology support and services to a number of hosted applications and databases.

1.7 System Environment

The NI GSS operates within the secure confines of the data center located within the OCC facility at 835 Brightseat Road, Landover, MD.

1.8 System Interconnection/Information Sharing

The OCC NI GSS provides the following interconnections with other information technology services.

- ATT Multi Protocol Label Switching (MPLS) Network
- Verizon Optical Network (VON) – Nortel Passport Switch
- ATT 800 Dial In from Denver District Office (Warm Site)
- Internet
- Westlaw
- Department of the Treasury
- Financial Management Service (Network)
- Financial Management Service (Mainframe Operations)
- Federal Deposit Insurance Corporation
- Federal Reserve Bank (Mainframe Operations)

2. PRIVACY IMPACT ASSESSMENT

2.1 FISMA System Privacy Threshold Analysis Determination Checklist

A *Privacy Threshold Analysis* is used by the Bureau's Privacy Act Officer to determine if a full Privacy Impact Assessment (PIA) is required for the system. (TD P 25-07, the Department of the Treasury, Privacy Impact Analysis Manual, dated July 2006 (Advanced Copy))

Y N Has a Privacy Threshold Analysis been completed?

Status of System

Y N This is a new development effort
Y N This an existing system

Personally Identifiable Information

The term *Personally Identifiable Information* refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to a specific individual.

Y N Does the system collect, maintain, and/or share information in an identifiable form (this includes information about government personnel, government contractors and consultants)?

If yes, please answer the following questions.

Y N Does the system contain information from or about the public?

Provide a general description of the way the system identifies an individual.

- The OCC NI GSS uses individual's first and last name in the email system to establish email accounts.
- Hosted applications contain PII as detailed in individual Privacy Impact Assessments.

What information does this system collect, maintain, or share?

- The OCC NI GSS uses individual's first and last name in the email system to establish email accounts.
- Hosted applications contain PII as detailed in individual Privacy Impact Assessments.

Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. (M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003)

Y N Has a Privacy Impact Assessment been completed?

- The NI GSS PIA is contained in the following sections.

2.2 Privacy Assessment

The following paragraphs detail the Privacy Assessment applicable to the OCC NI GSS.

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

Y N

2.2.2 Does the public have access to the system?

Yes, but only to the OCC public site on the World Wide Web. National banks have access by registration and certification to BankNet, the OCC extranet site, but are restricted to read/print access for information about their particular national bank.

2.2.3 Has a PIA been done before?

Y N

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

Y N Has a Privacy Impact Assessment been completed?

- A previous PIA was conducted and accepted/signed on July 24, 2004.

2.2.5 Has the system changed since the last PIA was performed?Y N **2.3 Data in the System/Application****2.3.1 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 GSS provides infrastructure for Information Technology (IT) capabilities provisioning to OCC employees, contractors, national banks and other financial regulatory entities at any given time in the present and future. This is a general support system that provides for the transmission of data from internal or external sources to the appropriate OCC system.

- The OCC NI GSS uses individual's first and last name in the email system to establish email accounts.
- Hosted applications contain PII as detailed in individual Privacy Impact Assessments.

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

- Employee and contractor information (names) are collected from individuals when the individual requests an email account within the OCC email system.
- Information on hosted applications PII is detailed in the individual application PIA.

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

- Information is NOT collected from any other source than the individual. Each individual is responsible for the accuracy of information submitted.
- Information collected in support of hosted applications is contained in the individual application PIA.

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

- Information Technology Service staff maintain the OCC NI GSS.
- The email system administrator has unrestricted access to email accounts for the purpose of maintaining and supporting the system, creating and deleting accounts, and performing restoration activities.
- All activities of the System Administrator (SA) are recorded and subject to audit.
- Other system operations and maintenance access is determined by enforcement of role based access controls and least privilege (limiting access to an absolute minimum necessary for mission accomplishment). Details are contained in the OCC NI GSS System Security Plan.
- Application SAs and database administrators (DBAs) are granted access to hosted major applications using least privilege and role based access controls (RBAC) that limit access to their specific major application and or associated database. Details are contained in individual application system security plans (SSP) and PIAs.

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

- Administrative Controls:
 - Position Descriptions detailing specific duties and responsibilities
 - Sensitivity Determinations
 - Least Privilege
 - Security (and Privacy) Awareness and Training
- Technological Controls
 - RBAC
 - Audit
 - Security Analysis and Reviews

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

- Individuals requesting email accounts within the OCC NI GSS are asked to provide their names to establish an email account. The application for an email account is voluntary, however if the individual does not provide their name, an individual email account cannot be established for them.
- Information regarding application acquisition of PII is contained in individual PIAs.

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

- Within the OCC NI GSS email system, accounts are active until the individual is no longer assigned or employed by OCC.
- When no longer required, accounts are deleted from the system by the email administrator.
- OCC maintains media sanitization procedures consistent with TD P 15-71 for electrical and optical storage devices. Devices are cleared, sanitized and checked for PII and SBU data before being reallocated to use by the system. Media devices that cannot be sanitized are destroyed using approved procedures detailed in TD P 15-71.
- Specific procedures for hosted applications are contained in individual application PIAs and SSPs.

2.4 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?

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 System of Records Report.

2.5 SOR Impact Evaluation

The OCC NI GSS is covered by one or more of the following System of Record Notices 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, and include

- 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 System of Records Notice is required in support of the OCC NI GSS. Any criteria marked with an “X” in the “Yes” column would indicate the likelihood of a *New or Altered System of Records Report* being required.

SORN Impact Evaluation Summary OCC NETWORK INFRASTRUCTURE GSS		
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		