Office *of the* Comptroller *of the* Currency

Ensuring a Safe and Sound Federal Banking System for all Americans.

Network Infrastructure - General Support System (NI-GSS)

Privacy Impact Assessment (PIA)

System Categorization: Moderate

Version 1.5

May 30, 2013

Prepared by:

Security & Compliance Services (SCS) and
Infrastructure and Operations (I&O)

DOCUMENT CHANGE CONTROL

VERSION	DATE	SUMMARY OF CHANGES	NAME
1.0	10/21/2008	Initial Working Draft	COACT Inc.
1.1	11/12/2008	Final	COACT, Inc
1.2	5/4/2009	Changes in approval requirements	IRM/Woodson
1.3	1/13/2011	Update /Review of Document	IRM/Curtis
1.4	10/16/2012	Update /Review of Document	ITS/I&O/Stewart
1.5	5/30/2013	Updated for Authorization	SCS

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:

Network Infrastructure (NI) General Support System (GSS)

1.2 RESPONSIBLE ORGANIZATION

Office of the Chief Financial Officer
Office of the Comptroller of the Currency (OCC)
400 7th Street, SW, Washington, DC 20024.

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) document

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:

Information Type	Confidentiality	Integrity	Availability
Services Delivery Support Information	Moderate	Moderate	Moderate
Rationale and Factors for Government Resource Management Information	Moderate	Moderate	Low
Disaster Management Mission Area	Low	Low	Moderate
Economic Development Mission Area	Moderate	Low	Low
Workforce Management Mission Area	Low	Low	Low

Information Type	Confidentiality	Integrity	Availability
Income Security Mission Area	Moderate	Moderate	Moderate
Litigation and Judicial Activities Mission Area	Moderate	Moderate	Moderate
Knowledge Creation and Management Mission Area	Low	Low	Low
Regulatory Compliance and Enforcement Mission Area	Moderate	Moderate	Low
Overall Per Category	**Moderate**	**Moderate**	**Moderate**
SYSTEM OVERALL	**MODERATE**		

1.5 SYSTEM OPERATIONAL STATUS

The system is currently **Operational.**

1.6 GENERAL DESCRIPTION/PURPOSE

The OCC NI GSS is a nationwide network facilitating the data processing needs of the OCC and supports OCC users throughout the country in carrying out their responsibilities to charter, regulate and supervise all national banks and federal savings associations.

It provides the hardware, software, program code and business logic to support the operation and management of the OCC's technology services. In addition, the NI GSS provides primary security services and data security mechanisms in support of OCC applications. These security services include Identification and Authentication (I&A), Logical Access Controls, and Auditing. Users employ the Identification & Authentication service when they first log into the network and then gain access to specific applications and general resources (e.g., network servers, network drives, print/file sharing, e-mail, intranet, and Internet access).

The NI GSS is essential to performing the OCC's mission. Without it, the supported major applications (MAs) and their missions would either be severely degraded or unable to function. This GSS supports the OCC in achieving its objectives, which are as follows:

- Ensure the safety and soundness of the national system of banks and savings associations.
- Foster competition by allowing banks to offer new products and services.

- Improve the efficiency and effectiveness of OCC supervision, including reducing regulatory burden.
- Ensure fair and equal access to financial services for all Americans.

The NI-GSS primary location is the Ashburn Data Center in Virginia.

1.7 SYSTEM ENVIRONMENT

The NI-GSS provides core and critical information technology support and services to OCC hosted applications and databases.

The OCC uses a Wide Area Network (WAN) to maintain Internet across the organization's many locations with a Local Area Network (LAN) in the individual buildings. The OCC maintains a dedicated nationwide network to its data center. The OCC WAN consists of an AT&T Multi-Protocol Label Switching (MPLS) telecommunications network that supports the transfer of data between Headquarters, the Data Center, four district offices, the Ombudsman's office and 96 field/bank offices. The Network Operating System (NOS) and workstation clients are Microsoft based. The network transport is industry standard TCP/IP which primarily supports a Microsoft networking infrastructure.

OCC data information is routed using OCC-owned equipment and does not travel through public networks. The OCC dedicated WAN telecommunication links are not encrypted. This vulnerability has been considered low risk because it would require accessibility to facilities, specialized equipment, and product specific expertise to monitor or access OCC data on WAN lines.

The main components of the environment included in this documentation are the:

- Physical Environment of the OCC Facilities (Data Center, Large Offices, Field Offices)
- Storage Area Network (SAN)
- Mainframe
- Server (non-specific)
- Client Systems (Desktops, Laptops, and Mobile devices)
- Network Perimeter Devices and Boundary Protection
- Remote Access Devices
- Active Directory (AD)
- File/print servers
- Database Management Systems
- Messaging (Exchange, Blackberry Enterprise Server)
- Citrix
- VM ware

1.8 FUTURE CHANGES TO NETWORK INFRASTRUCTURE (GSS)

There are currently no future changes planned for the NI GSS.

1.9 SYSTEM INTERCONNECTION/INFORMATION SHARING

The OCC NI GSS includes several interconnections with other information technology services. For Technical Detail see the OCC NI GSS System Security Plan.

2. PRIVACY IMPACT ASSESSMENT

2.1 PRIVACY ASSESSMENT

The following paragraphs detail the Privacy Assessment applicable to the Network Infrastructure (GSS).

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 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 GSS 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.

2.2.2 Why is the information being collected?

Employee and contractor information (names) are collected from individuals when the individual requests an email account within the OCC email system. This information is collected for purposes of user identification and authentication.

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

Information is NOT collected from any other source than the individual.

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

Each individual is responsible for the accuracy of information submitted. Information collected in support of hosted applications is contained in the individual application PIA.

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

- Information Technology Service (ITS) staff maintains 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.

2.2.6 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
  - Role Based Access Control
  - Audit
  - Security Analysis and Reviews

2.2.7 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.

2.2.8 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 FISMA Systems are contained in individual application PIAs and SSPs.

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 (OMB) 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.

The OCC NI GSS is covered by one or more of the following System of Record Notices as published in the Federal Register / Vol. 77, No. 64 / Tuesday, August 3, 2012 / Notices.

2.4 SECURITY ASSESSMENT AND AUTHORIZATION (SA&A)

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

Yes ☒ No ☐

Date ATO granted: **05/30/2013**