Office *of the* Comptroller *of the* Currency

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

Summation Enterprise

Privacy Impact Analysis

System Categorization: Moderate

Version 1.0

October 29, 2013

Prepared by:

Security & Compliance Services (SCS)

DOCUMENT CHANGE CONTROL

Version	Date	Summary of Changes	Pages Affected	Changes Made By:
1.0	October 29, 2013	Final version	All	SCS

Purpose

The Privacy Impact Assessment (PIA) is completed as a mandatory step in the authorization 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.

Do not include any Sensitive Information in the PIA. When finalized, the PIA will be a publicly-accessible document posted to the OCC public-facing website.

Questions regarding this PIA template should be directed to the OCC Privacy Act Officer for response.

NOTE

This document was prepared in support of the system's Security Assessment and Authorization (SA&A) 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

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:

Summation Enterprise, SUMENT

2.2 Responsible Organization

Chief Counsel's Office
Office of the Comptroller of the Currency (OCC),
400 7th Street S.W.
Washington, DC 20024.

2.3 Information Contact(s)

Names of person knowledgeable about the system, the system and data owner, security personnel, etc:

Key System Contacts (include name, phone, and email):
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:

Information Type	Confidentiality	Integrity	Availability
Corrective Action *Mission Area:* Controls and Oversight	Low	Low	Low
Personal Identity and Authentication *Mission Area:* General Government	Moderate	Moderate	Moderate
Information Security *Mission Area:* Information and Technology Management	Low	Moderate	Low

Judicial Hearings *Mission Area:* Litigation and Judicial Activities	Moderate	Low	Low
Legal Investigation *Mission Area:* Litigation and Judicial Activities	Moderate	Moderate	Moderate
Legal Prosecution and Litigation *Mission Area:* Litigation and Judicial Activities	Low	Moderate	Low
Overall Per Category	Moderate	Moderate	Moderate
System Overall	Moderate		

2.5 System Operational Status

Summation Enterprise is currently Operational.

2.6 General Description/Purpose

Summation Enterprise, an Access Data product, is a litigation software suite used to complete investigation and litigation-related tasks. The software allows for searching, retrieving, coding/annotating, and organizing information and producing electronically stored information responsive to discovery requests.

2.7 System Environment

Summation Enterprise is a commercial off the shelf client server system that resides on Microsoft (MS) Windows 2008 R2 Server, MS Windows 2008 SQL Server, and MS Operating System workstations. Summation Enterprise is available only to authorized users employed by the OCC.

2.8 Future Changes to Summation Enterprise.

There is a planned upgrade to Summation Enterprise Pro.

2.9 System Interconnection/Information Sharing

Through discovery requests and subpoenas, relevant subject matter information is shared with third parties, appropriate government or self-regulatory organizations, the

Department of Justice, an adjudicative body, individual or entity directly involved in the legal proceedings, and Congressional offices.

3. PRIVACY IMPACT ASSESSMENT

3.1 Privacy Assessment

The following paragraphs detail the Privacy Assessment applicable to Summation Enterprise

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 ☒

3.2 Data in the System/Application

3.2.1 What elements of PII are collected and maintained by the system?

The system may collect and store any information obtained as part of investigations and other legal activities. The collected information is in various electronic and non-electronic formats such as word processing files, spreadsheets, databases, emails, images, audio files, videos, and boxes of paper documents. This information may contain sensitive information of many types including personally identifiable information (PII). For example, during an investigation, the OCC may obtain financial transaction data, loan data, banking records, employee records, and email records that may contain PII such as names, addresses, telephone numbers, email addresses, birth dates, Social

Security numbers / tax ID numbers, bank account numbers, loan account numbers, credit card numbers, and other personal information.

3.2.2 Why is the information being collected?

The information is being collected as part of the agency's law enforcement and other activities, such as investigating compliance with financial statues and regulations; investigating internal matters and representing the OCC interests in legal actions and proceedings.

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

Information is provided from individuals, such as whistleblowers and consumers, entities involved in legal proceeding or investigations, OCC-regulated institutions, and governmental, tribal, self-regulatory or professional organizations.

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

Appropriate security and chain-of-custody controls protect information from loss and ensure the content remains unchanged from the time it was obtained. Controls include the use of forensic tools to verify information has not been changed.

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

OCC employees authorized by the Litigation or Enforcement and Compliance directors (i.e. the data owners) will have access to the respective litigation cases or investigations. The authorized OCC employees include attorneys, paralegals, legal support staff, assisting examiners, case managers and IT system support.

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

Physical media containing source information is secured at the OCC headquarters building. To enter the building, employees must present authorized federal government SmartID cards to private security guards at building entrances. Headquarters visitors are checked in by private security guard, undergo a hand-held metal detector screening, a visual inspection of their packages; and require an employee escort at all times. Under security guard supervision, card readers control the gated entrance to the OCC building space. Within the OCC building space, the source information physical media is stored in locked cabinets within a locked law department room.

System information is secured by OCC network account authentication, Active Directory Security Group membership, and group membership internal to the system.

Summation Enterprise application servers and data storage reside at the OCC's data center in Virginia.

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

Individuals who provide information on a voluntary basis can choose not to provide information. Data collected from other systems, email for example, will not offer individuals an opportunity to decline. Individuals do not have a right to decline to provide information that is required by law such as compulsory process.

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

Records are retained in accordance with the OCC's records management policies and National Archives and Records Administration regulations. Case files are destroyed 15 years after the case is closed.

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 ☒

Treasury/CC.510 covers the category of individuals and the types of records in Summation Enterprise.

3.4 Assessment and Authorization

Has the system been assessed and authorized within the last three years?

Yes ☒ No ☐

Date ATO granted 10/29/2013