Change History – Order Management System (OMS II) Privacy Impact Assessment (PIA)				
Version Number	Version Date (mm/dd/yyyy)	Change Description/Purpose		
		Figure, Table, or Paragraph Number	A M D	Title or Brief Description
v.1.0	05/13/2014		A	Initial "Draft" issuance of PIA.
v.1.2	06/30/2014	Throughout document.	M	Where appropriate changed "user" to "customer".
v.1.2	06/30/2014	Question 1- System Application/General Information. Question 1- Data in the System	D	Deleted duplicative section regarding collection of information about service provider employees, sub-contractors, Federal employees and government contractors.
v.1.2	06/30/2014	Question 2- Data in the System	M	Changed wording "If cookies are disabled, the information will be kept anonymous so it cannot be associated with any particular user, IP address, or other PII."
v.1.2	06/30/2014	Question 4- Data in the System	M	Updated verbiage to clarify IP address truncation for non-registered customers.
v.1.2	06/30/2014	Question 9- Maintenance and Administrative Controls	M	Language changed to reflect updated content in M-10-22 Q&A and Privacy Policy.
V.1.2	07/2/2014	Throughout document.	D	Removed Remember Me option per 7/1/2014 meeting.
V.2.0	08/01/2014	Throughout document.	M	Updated per Department of Treasury review.
V.2.1	08/03/2014	Throughout document.	M	Addressed PTR comments, corrected citations, minor suggested changes for consistency of terminology, and legal review for GLER concurrence.
V.2.2	08/04/2014	Throughout document.	M	Addressed OPTR and General Counsel comments, accepted proposed changes.
V2.3	08/05/2014	Introduction #1 and Table 1	M	Changed the name of the system to OMS II and removed the reference to project. Added a row to address Google Analytics.

A - ADDED **M** - MODIFIED **D** - DELETED

***This change log does not detail grammatical or editorial changes.

Privacy Impact Assessment

Introduction

1. ***Name of System:***
   eCommerce End-to-End Solution: Order Management System II (OMS II)

2. ***Purpose of the System:***
   The United States Mint is replacing the current Integrated Retail Information System so the bureau can continue to conduct its numismatic sales in a productive, reliable and secure manner. The United States Mint has contracted with a full service provider to meet the electronic commerce ("*eCommerce*") needs of its retail sales operations. OMS II is replacing the current outdated system and is expected to provide significant improvement over the current system's functionality and durability. The OMS II service provider will maintain and operate all required system hardware and software components with oversight from the United States Mint. OMS II supports the bureau's numismatic operations and is intended to provide United States Mint customers with an experience that keeps pace with advancements in both technology and functionality increasingly prevalent in other retail settings. OMS II provides a full suite of applications that perform *eCommerce*, retail order management, warehouse management, customer service, interactive marketing services, payment processing, all information technology infrastructures, and other ancillary functions in an effort to provide the general public with United States Mint products and services in a cost-effective and efficient manner. This Privacy Impact Assessment only covers information in OMS II (i.e., information that is collected via the United States Mint's online store) and does not cover the entire United States Mint informational website which is maintained separately.

3. ***Will the system be (or is it now) a Major Information System[1]?***
   Yes.

4. ***Under which SORN(s) does the system/application operate, if any? Provide name(s) and number(s).***
   Treasury/ United States Mint - .009 – Order Management System (OMS) (*replacing* United States Mint .009, "Retail Sales System").

[1] "Major information system embraces 'large' and 'sensitive' information systems which means a system or project 'that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.'" OMB Circular A-130, para. 6u.

A. <u>Contact Information:</u>

1. Who is the person(s) completing this document?

- Lauren Buschor, Chief Information Officer (CIO), Information Technology Department (ITD), United States Mint
- Rick Skorny, Executive Lead, United States Mint

2. Who is the system developer/analyst?

OMS II is a turn-key *eCommerce* service that will be configured and customized according to the requirements of the service provider's contract with the United States Mint. It was developed by the United States Mint under contract with PFSweb, Inc. When implemented for the United States Mint, OMS II will include the contents of existing databases of United States Mint customers previously developed by the United States Mint.

3. Who is the system owner?

Associate Director of Sales and Marketing, United States Mint (currently Marc Landry (Acting)).

4. Who is the system manager?

DeAnna Wynn, Deputy CIO, ITD, United States Mint.

5. Who is the Information Systems Security Manager who reviewed this document?

Ray Hardy, Chief Information Security Officer, ITD, United States Mint.

6. Who is the Bureau Privacy Act Officer who reviewed this document?

Kathleen Saunders-Mitchell, Disclosure Officer, United States Mint.

7. Who is the IT Reviewing Official?

Lauren Buschor, CIO, ITD, United States Mint.

B. <u>System Application/General Information:</u>

1. Does this system contain any personal information about individuals[2]?

---

[2] Such as Personally Identifiable information (PII): PII may include but is not limited to: Information relating to race, national or ethnic origin, religion, age, marital, or family status; Information relating to education, medical, psychiatric, psychological, criminal, financial, or employment history; any identifying number (such as a Social Security number), symbol, or other particular assigned to the individual; and name, address, telephone number, fingerprints, blood type, or DNA.

As used in this PIA, the term PII also encompasses "Information in Identifiable Form (or data)." As defined in OMB Memorandum M-03-22, PII is information in an IT system or online collection that (i) directly identifies an individual (e.g., name, address, Social Security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). In the E-Gov Act § 208(d), "identifiable form" is defined as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." Under the E-Gov Act § 208(b)(1)(A)(ii)(II), the term "identifiable form" also "includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been

OMS II includes 16 applications or services that capture and reuse the information provided by the customer through the public-facing online store, phone, mail orders and retail points of sale.[3] These data are used to verify shipping and billing address information, conduct fraud checks and support targeted marketing efforts by enhancing the overall customer experience, in addition to fulfilling customer orders.

The following table describes the functions that each of the 16 applications or services perform as part of OMS II. These 16 applications are included in the PFSweb's hosted system, and the data are used solely by (1) United States Mint to carry out its mission, and (2) PFSweb to carry out its contractual obligations to United States Mint.

Table 1 – OMS II Application Descriptions

Application/Service Name	Description
AgilOne Omni-Channel	This application allows the United States Mint to conduct sales analysis and create targeted marketed campaigns.
CyberSource	This service assesses the fraud risk of each credit card transaction using a set of business rules that identify characteristics of fraud and similarity to prior fraudulent transactions. Transactions that exceed the threshold for risk are flagged for manual review.
Demandware	This service manages all of the content and web screens for the online store. It is also used by the customer service representatives to place orders on behalf of phone customers.
Exact Target	This application supports the creation and management of email marketing campaigns by the United States Mint. Also sends all transactional email as triggered by Demandware and the Order Management Application Suite.
ForeSee Survey	A survey utility that polls a sampling of customers to rate their customer experience and level of satisfaction.
Google Analytics	This application is not part of PFSweb's solution, but is used by the United States Mint to track visit statistics to all United States Mint websites including the online store. There is no PII collected by Google Analytics.
IBM Digital Analytics	This application gathers online store browsing trends of United States Mint customers and visitors to support sales analysis. Also includes comparative benchmarks about industry peers.

posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government."

[3] Retail points of sale only include sales made directly by the United States Mint to the public. It does not include private companies that purchase products from United States Mint and resell them to the public (i.e., Aramark).

Application/Service Name	Description
iCommerce Agent (iCA)	An application that allows customer service representatives to research customer inquiries and take phone orders.
iCommerce Product Content Mgmt (PCM)	This application allows centralized management of United States Mint product content that supports the online store and retail points of sale. It provides tools to manage structured data, product photography, and any other rich media assets.
iCommerce Subscriptions (iCS)	This application enables customers to create numismatic product subscriptions/enrollments. This application creates scheduled orders based on subscriber preferences.
Live Chat	This application enables customers to communicate with customer service representatives via interactive chat.
NCR CounterPoint	Point-of-sale software used at retail points of sale, such as mobile and over-the-counter sales.
Order Management Application Suite	The core part of OMS II that stores, processes, and supports fulfillment of the orders. Includes the accounting functions, warehouse management system, and the secure data repository (SDR) for credit card data.
Reports Portal	This application allows employees to access and generate reports including sales figures, online store visits, and system performance and usage.
SDR	Stores credit card information used by the Order Management Application Suite. The information is encrypted and is only accessible via the Order Management Application Suite.
Symago	This application allows customers to use interactive voice response prompts as an alternative to speaking with a customer service representative. For example, it allows them to inquire about existing orders by using automated phone menus.
Uptivity	The application is a voice call and screen captures recording application for the contact center for quality monitoring and management by the United States Mint, as well as coaching and dispute resolution.

The below table summarizes how each application and service within OMS II handles PII. In all cases, PII collection, storage, and use will comply with OMB Memorandum M-10-22. Under no circumstances will these applications or services be used to track individual-level activity on the Internet outside of OMS II; to share the data obtained, without the customer's explicit consent, with other departments or agencies; to cross-reference, without the user's explicit consent, any data gathered against PII to determine individual-level online activity; or to collect PII without the customer's explicit consent in any fashion.

In the table below, the following columns are included:

- *"Originates Collection of PII?"*- Collects and stores PII provided directly by the public. (Refer to Data in the System, question).
- *"Stores Copy of PII?"*- Utilizes PII through interfaces with other OMS II applications or services. (Refer to Data in the System, question 2a).
- *"Derives/Aggregates PII?"*- Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information. (Refer to Attributes of the Data, question 2).

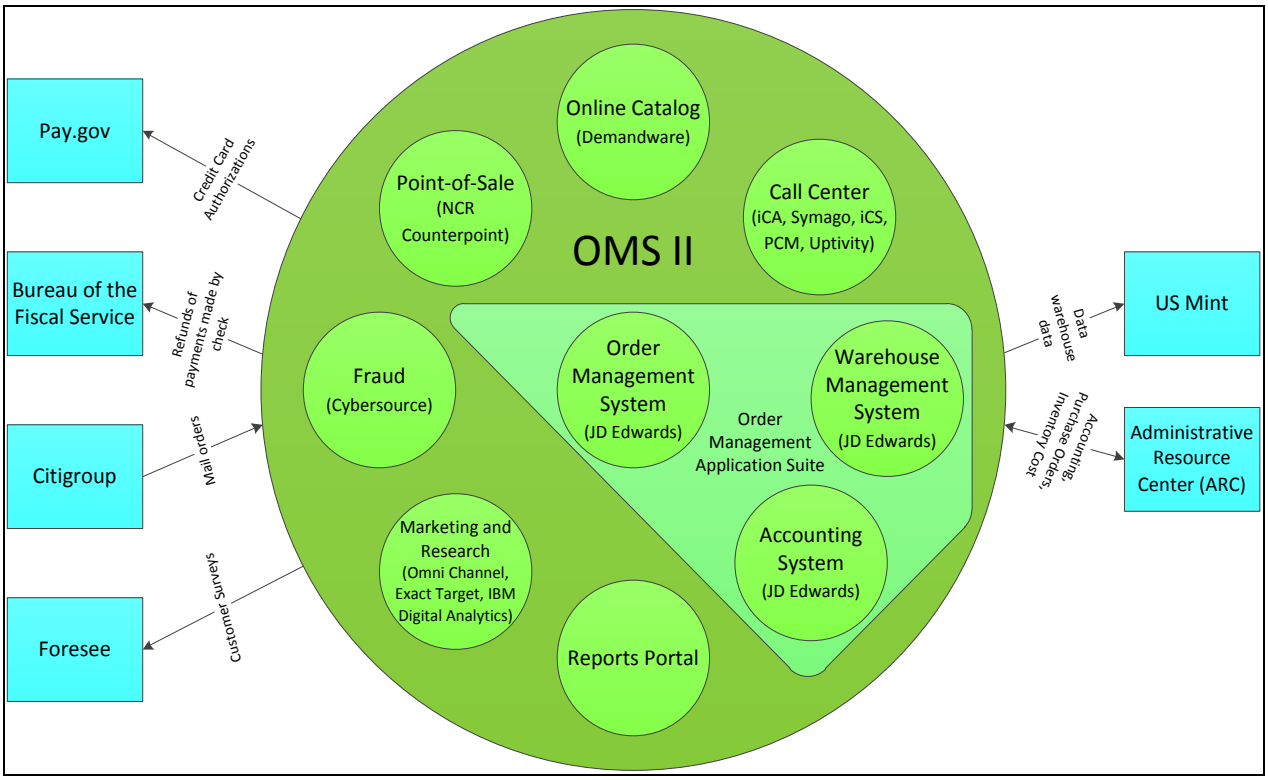
Table 2 – OMS II PII Storage or Usage

Application/Service Name	Originates Collection of PII?	Stores Copy of PII?	Derives/ Aggregates PII?
AgilOne Omni-Channel	No	Yes	Yes
CyberSource	No	Yes	Yes
Demandware	Yes	No	No
Exact Target	No	Yes	Yes
ForeSee Survey	No	No	No
IBM Digital Analytics	No	Yes	Yes
iCommerce Agent (iCA)	Yes	Yes	No
iCommerce Product Content Mgmt (PCM)	No	No	No
iCommerce Subscriptions (iCS)	No	Yes	Yes
Live Chat	Yes	No	No
NCR CounterPoint	Yes	No	No
Order Management Application Suite	No	Yes	No
Reports Portal	No	No	No
Secure Data Repository (SDR)	No	Yes	No
Symago (IVR)	No	No	No
Uptivity	Yes	No	No

OMS II also collects and stores Federal employee, government contractor employee, and subcontractor employee user information, such as user name/ID and system usage tracking. In some cases, OMS II will log the files accessed by a PFSweb employee or subcontractor employee. These audit logs are stored and periodically reviewed to ensure access to data is restricted on a need-to-know basis and to verify the integrity of the information collected and stored. It is therefore necessary to ensure the security and privacy of customer information.

The following diagram shows a simple view of how the applications and services form OMS II.

Figure 1 – OMS II Context Diagram



2. ***What legal authority authorizes the purchase or development of this system/application?***
   31 U.S.C. §§ 5111(a)(3) (authorizing the United States Mint to "prepare and distribute numismatic items") and 5136 (establishing the United States Mint Public Enterprise Fund for "receipts from Mint operations and programs, including the production and sale of numismatic items, the production and sale of circulating coinage").

3. ***How is privacy addressed in documentation related to system development, including statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and especially the initial risk assessment?***
   OMS II processes and transmits sensitive but unclassified data, which requires protection for confidentiality, integrity, and availability. Sensitive data consist of mission essential information; financial and budgetary information, including that covered by the Trade Secrets Act; personal information pertaining to customers and organizations protected by the Privacy Act of 1974 and/or exempt from disclosure under the Freedom of Information

Act; procurement-sensitive information; customer financial information; and security-related information.

Privacy concerns will continue to be addressed as a requirement throughout the lifecycle of OMS II. Procurement agreements require the service provider to develop, modify, and/or maintain OMS II to ensure continued compliance with the Privacy Act of 1974, Treasury Directive 87-05 ("Electronic Commerce Initiatives"), the United States Mint's privacy policies and directives, and other federal laws, policies and regulations, including those with privacy provisions.

PFSweb undergoes annual security compliance reviews based on proprietary information security standards for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and point-of-sale cards.

C. Data in the System:

1. What categories of individuals are covered in the system?

OMS II maintains information about members of the public who make purchases using the United States Mint's public-facing online store or order by phone, mail orders or retail point of sale. It also includes individuals who receive gifts from someone who orders via one of these methods of purchase. It may also include information regarding representatives of bulk or term customers who purchase products and services from the United States Mint. This also includes individuals who request to be added to United States Mint mailing or email lists to receive promotional or educational materials (an option available to anyone who visits the online store, whether or not they make a purchase). To register for an online shopping account, to make a single transaction purchase, or to be added to these mailing or email lists, a customer must provide PII (e.g., his or her name, mailing address, telephone number, password and security question response, or e-mail address); in accordance with our Terms of Service, by providing this PII, the customer is also warranting that he or she is 18 years of age or older. Registered customer accounts require verification of age to ensure compliance with the Children's Online Privacy Protection Act (COPPA). (Note: COPPA restricts operators of websites in their interactions online with children under the age of 13; however, the United States Mint has a long-standing rule of restricting access to customers over the age of 18 by deeming that a customer's submission of any PII—such as his or her email address, name, or postal address—means that he or she is warranting that he or she is 18 years of age or older). Purchases made without registering (as a guest) rely on the purchasers' complying with prepared age-limitation notices to ensure compliance with COPPA.

OMS II also collects and stores Federal employee, as well as government contractor and subcontractor employee, user information such as user name/ID and system usage tracking. In some cases OMS II will log and review the files accessed by a PFSweb employee or subcontractor employee to ensure access to data is restricted on a need-to-know basis and to verify the integrity of the information collected and stored.

2. What are the sources of the information in the system?

OMS II collects PII from the following individuals:

(1) Nonregistered Online Visitors ("*Nonregistered Visitors*"). These are individuals who visit the United States Mint's online store, but do not register for an online shopping account or make any purchases. Certain information is automatically collected from all *Nonregistered Visitors* to the online store using cookies (files that are placed on a website visitor's computer to track and collect information). If *Nonregistered Visitors* go to the online store (without first disabling first-party cookies) solely to read or download information—and do not, for example, send e-mail to the United States Mint or complete an online form or opt-in to certain data collections and uses (by purchasing online, creating an account or subscribing to a newsletter)—the United States Mint collects and stores only the following information:

- Networking: the domain used to access the Internet and connection speed;
- When/Where: the date, time, and region from which the online store was accessed;
- Content: pages visited and files downloaded in the online store;
- Referrer: the Internet address of a website that may have referred or linked the visitor to the online store; and
- Device/Browser: the user's browsing habits while in the online store (but not on the rest of the United States Mint's website or other sites to which the user navigates after leaving the online store), and other technical information about the computer or device used to access the online store (e.g., operating system, screen resolution and color, Flash/Java support, language).

When *Nonregistered Visitors* navigate to the United States Mint online store without disabling first-party cookies, they are assigned an auto-generated visitor identifier to track their browsing behavior while they remain in the online store (the tracking ends if the *Nonregistered Visitor* leaves the online store and navigates to other parts of the United States Mint site or to other sites). The United States Mint automatically collects the geo-location data contained in the first six digits of the internet protocol (IP) address ("truncated" [not the full] IP address) and device settings. IP addresses allow a website (e.g., the United States Mint's online store) to recognize the device when the device owner visits the site. Because the truncated IP address reveals only broad geo-location data (i.e., a particular region), it is not PII. This information is collected whether or not an individual who navigates to the online store is a *Registered Customer* or has logged into his or her customer profile. The information is used to improve the online store based on behavioral analysis (products viewed, pages browsed, previous order history and purchasing habits) and is not associated with any PII. United States Mint online store customers can disable this technology by disabling cookies in their web browser settings before navigating to the online store.

(2) Registered Online Shopping Account Customers ("*Registered Customers*"). The United States Mint provides customers the option of creating a registered account. These *Registered Customers* are individuals who visit the United States Mint's online store, register for an account and make purchases online. The following PII is collected during registration: name (first and last), physical address, phone number, email address, login name, password, product and communication preferences, billing and delivery address (including country, city, county, state and zip code), order history and credit card payment information. In accordance with our Terms of Service, by providing this PII, the customer

is also warranting that he or she is 18 years of age or older. *Registered Customers* are also required to select and answer one of many security questions available.

If customers wish to register to create an online shopping account, the United States Mint also requires that they explicitly agree (i.e., opt in) to have their full IP address (not merely the truncated [geo-location] version collected for online store *Nonregistered Visitors*) and their browsing activities tracked within the online store and associated with other information they provide to the online store. The full IP address is PII because it can conceivably be traced to an individual when combined with other information (e.g., information from the Internet service provider regarding the account holder from whom the IP address originated, plus additional information from the owner of the account). The online store uses cookies (files placed on a website visitor's computer to allow interaction with the site) to track and collect the user's browsing and purchasing habits and activities. The *Registered Customer's* browsing habits are tracked using a persistent cookie that associates the customer's PII (name, billing and shipping address, phone number, email address, payment, birth month, and credit card information, product and communication preferences and order history) with his or her browsing and purchasing behavior.

Both *Registered Customers* and *Unregistered Online Single Transaction Customers* (see below) may typically pay for products purchased in the online store using credit cards, wire transfers, invoice payments, and inter-agency funds transfer. Only credit card transactional information is collected and stored in OMS II. Information necessary to make purchases using other methods of payment is stored in other systems. OMS II merely receives notice that payment was received (e.g., the United States Mint Finance Department is notified of successful payment by the banking institution after payment by wire transfer).

For United States Mint customers who already have an existing online shopping account when the United States Mint launches OMS II, the United States Mint will invite each of these customers to confirm his or her registration by explicitly agreeing (i.e., opting in) to become a *Registered Customer* in OMS II and to create a new password to maintain access to his or her account and account services. To do this, customers will need the answer to their security question that they provided when they first registered for an account on the online store.

(3) Unregistered Online Single Transaction Customers ("*Single Transaction Customers*"). Customers do not need to create an online shopping account to make an online purchase. To make an online purchase of any kind (*Registered Customer* or *Single Transaction Customer*), the United States Mint requires information such as the customers' credit card data, and telephone number, name, and e-mail and postal addresses for customers or their recipient. In accordance with our Terms of Service, by providing this PII, the customer is also warranting that he or she is 18 years of age or older. When *Single Transaction Customers* make a purchase, they are opting-in to certain collections and uses of their browsing and personal information.

Single Transaction Customers, like *Email Subscribers* and *Registered Customers*, must explicitly agree (i.e., opt in) to have their full IP address (not the truncated version collected for *Non-Registered Visitors*) and their browsing activities tracked within the online store and associated with other information they provide to the online store. Their browsing habits are tracked using a persistent cookie that associates their PII (First name, last name, telephone number, email address, billing address, shipping address, credit card information, (including expiration date and security code) credit card data) with their browsing and purchasing behavior. A customer's browsing habits will be associated with additional types of PII if the *Single Transaction Customer* also conducts other transactions in the online store (e.g., becomes an *Email Subscriber*).

(4) Online Customers Who Choose to Use United States Mint Customer Assistance Services ("*Online Assistance Customers*"). These are customers who choose to use certain information services available in the online store (assistance by email or chat assistance). Visitors to the online store do not necessarily need to create an account or make a purchase to use these services and many of the United States Mint's other online services. For example, some online visitors may seek assistance by email or chat assistance, yet decline to make a purchase. These individuals are labeled as "customers" under this heading even if they never choose to purchase any products using the United States Mint's online store. To use the email and chat assistance features (whether or not the visitor makes a purchase), the United States Mint will require information such as the customer's name and email address.

(5) Online Visitors Who Subscribe to Email Communications from United States Mint ("Email Subscribers"). Online visitors have the option of becoming *Email Subscribers* to receive e-mail communications (promotional/informational newsletters) from the United States Mint with general information about its products and services. *Email Subscribers* can (but need not) be customers who purchase products and services from the United States Mint. When a visitor becomes an *Email Subscriber*, the United States Mint collects information including the *Email Subscriber*'s name, e-mail address, birth month, and browsing activities. In accordance with our Terms of Service, by providing this PII, the customer is also warranting that he or she is 18 years of age or older.

Email Subscribers, like *Registered Customers* and *Single Transaction Customers*, must explicitly agree (i.e., opt in) to allow their browsing activities to be tracked and associated with other information they provide to the online store. Their browsing habits are tracked using a persistent cookie that associates their PII (name, e-mail address, and birth month) with their browsing and purchasing behavior. Please note that the browsing habits will be associated with additional types of PII if the *Email Subscriber* also conducts other transactions in the online store (e.g., becomes a *Registered Customer*).

(6) Third-Party Recipients of Gifts from Mint Online Customers ("Gift Recipients"). Both *Registered Customers* and *Single Transaction Customers* have the option of making gift purchases on behalf other individuals. Because of the nature of online gift transactions, certain information must be collected regarding the recipient to deliver the product as requested by the customer making the purchase on the recipient's behalf. The United

States Mint collects and stores information received from the customer about third-party gift recipients. For gifts, the customer must provide the recipient's shipping information (including first name, last name, and shipping address) to complete the order transaction and product delivery. Gift recipient information is used solely to deliver purchased product(s).

(7) Offline Transaction Customers. In these transactions, personal information is collected directly from the purchaser in person at a retail point of sale, by mail services, or through telephone by customer service representatives. Customer service representatives follow standard procedures while collecting personal information from the customer over the phone; phone calls will be recorded for quality assurance and training purposes. Prior to recording phone calls, customers are notified that the phone call may be recorded and they may choose to disconnect at any time.

(8) Visitors or Customers Who Submit Email. If visitors or customers choose to submit an email comment or inquiry through the United States Mint's "Contact Us" page or request a print catalog (of the products sold in the online store) to be sent by postal mail, the United States Mint may collect personal information such as customers' names, e-mail and home addresses, and telephone numbers.

(9) Visitors or Customers Who Complete Online Surveys. If customers choose to complete an online survey, the United States Mint and its contractors collect and store responses anonymously (the customer cannot be identified with the survey response). The United States Mint uses this information to learn about its customers and to improve its website, and its products and services generally. Customers are not required to complete any survey to use any feature of the United States Mint's website, including its online shopping features.

(10) Logs to Monitor Employees and Contractors Who Have Access to OMS II. OMS II also collects and stores Federal employee, as well as government contractor and subcontractor employee, user information such as user name/ID and system usage tracking. In some cases, OMS II will log the files accessed by a PFSweb employee or subcontractor employees.

2a. Is the source of the information collected directly from the individual or is it taken from another source? If not directly from the individual, then from what other sources could the information come?

Information is collected directly from the individual, except in the case of gift recipients, whose information—name, shipping address —is collected from the purchasing customer and stored in a record created for the gift recipient in a similar manner as directly-provided customer information.

OMS II also tracks and stores Federal employee, as well as government contractor and subcontractor employee, information to include user name and logged activity within OMS II. OMS II activity logging is outlined in user employment agreements, in federal government contracts, and user rules of behavior that are provided to all system users

prior to granting access; this data is stored within OMS II separately from numismatic customer information.

2b. What Federal agencies, if any, are providing data for use in the system?
External Federal agencies do not provide information to OMS II. OMS II receives inventory-related information within the Department of the Treasury from the Bureau of the Fiscal Service (Administrative Resource Center) and payment authorizations from Pay.gov (also operated by the Bureau of the Fiscal Service).

2c. What State and/or local agencies, tribal governments, foreign governments or international organizations, if any, are providing data for use in the system?
No state and/or local agencies provide data for use in OMS II.

2d. From what other third party sources will data be collected, if any?
The United States Mint regularly uses rental email (e.g., Yahoo, Google) and mailing lists from third-party organizations, such as designated recipient organizations (e.g., National Baseball Hall of Fame, United Negro College Fund, March of Dimes) that are eligible for the payment of surcharges on the sales of commemorative coins; data from these lists will be collected in OMS II for promotional purposes. Recipient organizations (identified by law) provide lists of potential customers who may be interested in purchasing commemorative coins. After initial outreach, the United States Mint uses the mailing or email address only if an individual chooses to do business with the United States Mint.

OMS II will use services for address validation and standardization. This allows the addresses entered by a customer or customer service representative to be validated against a common list of postal service-defined addresses and the system will provide standardized address options for user selection.

Domain name services are used to resolve locations of IP addresses which are collected for fraud protection and marketing purposes. The location assists the United States Mint's efforts by allowing browsing and purchasing history to be aggregated by broad geo-location.

Mail orders are submitted to the lockbox designated for the United States Mint; this customer information is then entered into OMS II for processing.

2e. What information will be collected from employees? And what will be collected from the public? (e.g., social security numbers, addresses, telephone numbers, badge numbers, user identifiers, credit card numbers, etc.)
The information that OMS II collects from PFSweb, United States Mint and contractor employees is as follows: (a) user information such as user name/ID, (b) OMS II activity, and (c) logging data of the files accessed by a PFSweb employees or subcontractor employees.

The information that OMS II collects from the public (i.e., customers and visitors to the site, which may include employees) is as follows: (a) name, (b) address, (c) phone number, (d) email address, (e) payment method and related information, as well as credit

card expiration date and credit card verification code, (f) communication preferences, (g) order or subscription/enrollment information, (h) IP address, and (i) browsing and purchasing history. Customers have the option to provide month of birth as part of their profile.

For additional information about the information OMS II collects from persons browsing on the United States Mint's store website, see section B, Question 1, and section C, Question 2, above.

4. Accuracy, Timeliness, and Reliability[4]

3a. How is data collected from sources other than from bureau records going to be verified for accuracy?

Except with respect to gift recipients, data are collected directly from the individual source via phone, retail point of sale, mail and/or online store. Credit card information is verified to ensure that the information provided for payment (e.g., name and address, three digit code, expiration date) matches the owner of the credit card.

Gift recipient information is provided by the purchaser. OMS II will utilize automated services for data address validation and standardization; the customer or customer service representative will have the ability to decline any automated recommendation for address validation or standardization.

Except for mailing and email address lists provided by recipient organizations (whose verification is typically provided by the list owner), the other data listed in 2b above do not include PII, nor are they used in conjunction with PII collected by the online store.

In cases in which data are collected via phone, the customer service representatives follow a standard procedure for reviewing and validating the information that is collected during the ordering process. Customer service representative procedures dictate that they must use the same application as the customer would. This ensures that information is inputted directly into OMS II and undergoes the same validation checks as if the customer inputted the information into the online store. Any validation errors will be addressed immediately during the customer interaction.

OMS II employs basic provisions for validating certain types of information, such as addresses and credit card numbers, based on required field input requirements and credit

[4] The Privacy Act requires that agencies make reasonable efforts to assure that such records are accurate, relevant, timely, and complete about individuals and maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination. These requirements are statutory and need to be addressed. If the data does not meet any one of these four components, then fairness in making any determination is compromised.

There must be documentation as to how the requirements are enforced while the data is retained in the system, and what data is considered sensitive. Maintaining metadata (documentation on the data) is important so that it can be referenced in the future to identify data conditions when making decisions about data from a system (OMB Circular A-130, para. 8.a.4.).

card domains. OMS II does not change data provided by a customer; however, if an address is matched or known, OMS II provides a suggestion for customer selection. Credit card information is confirmed by the credit card processor.

3b. Is completeness required? How will data be checked for completeness?
To process a purchase or product subscription and/or successfully fulfill a customer's order, OMS II requires a minimum set of information (purchaser name, address, telephone number, billing and recipient shipping address, and credit card, check or wire transfer processing information). All mandatory fields must be completed before the customer can move to the next page when registering or making a purchase. Similarly, to process a request for agency communications, such as electronic newsletters or product and promotion notification, the system requires the subscriber to provide his or her name and email address. Customers cannot opt-out of transactional email; this information is already gathered during the checkout process. Any additional information requested through online, mailed or point of sale interactions are optional. Therefore, the failure to populate these fields does not affect the completeness of the information in OMS II.

In cases in which data are collected via phone, customer service representatives receive training to ensure completeness of orders while protecting customer PII. This includes ensuring the completion of all required fields before finalizing the transaction.

3c. Is the data current? What procedures will ensure this?
The currency of the data is dependent upon the information the customer or rental list owner provides and how often they update registration information or make purchases. If an order cannot be processed, reasonable efforts will be undertaken to contact the customer to rectify the issue and any associated data discrepancies (e.g., bounced emails, returned mail order catalog).

The address validation database is updated on a quarterly basis from the United States Postal Service to capture any recent address changes; however, customers can at any time decline to use the results of the address validation checks. Additionally, list rental agreements typically contain verification warranties.

Registered Customers may update their account information at any time (thus keeping it current). *Information required to complete a sale is verified every time a Registered Customer* or *Single Transaction Customer* makes a purchase because changes must be made by the customer to ensure accurate delivery and to verify payment information.

3d. Are the data elements described in detail and documented?
Yes.

If yes, what is the name of the document?
All PII data elements are documented in PII Checklists completed by the vendor for all applications that collect PII for use in OMS II. The information contained in these checklists is summarized in Table 3.

Table 3 –PII Collected by Each OMS II Application

PII Types	AgileOne	CyberSource	Demandware	ExactTarget	IBM	iCA	iCS	Live Chat	NCR-POS	OMS	SDR	Uptivity
Name	x	x	x	x		x	x	x	x	x		x
Gender	x		x			x	x					
Birth Date	x		x	x								
Home Physical Mailing Address	x	x	x		x	x	x	x		x		x
Personal Cell Number	x	x	x			x	x	x		x		x
Personal Home Phone or Fax Number	x	x	x			x	x	x		x		x
Personal e-mail address	x	x	x	x	x	x	x	x	x	x		x
Education Information			x									
City or County of Birth			x									
Mother's Maiden Name			x									
Network communications data								x				
Device setting or preferences (e.g., security level, sharing options, ringtones).					x							
User names, avatars etc.	x		x			x	x		x			x
Credit Card Number		x	x								x	x
Internet Protocol Address (IP) Address (where known to belong to an individual or unknown whether the IP address belongs to an individual or organization)	x	x	x		x			x				
User ID assigned to a user of Treasury IT	x	x	x	x	x	x	x		x	x	x	x
Date and Time an individual accesses a facility, system or other IT	x	x	x	x	x	x	x		x	x	x	x
Files accessed by a user of Treasury IT	x		x	x	x	x	x		x	x	x	x
Contents of files accessed by a user of Treasury IT	x		x	x	x	x	x			x		x

4. What opportunities do individuals have to <u>decline</u> to provide information (i.e., where providing information is voluntary) or to consent to particular uses of information (other than required or authorized uses)?

Nonregistered Visitors may decline to provide PII when browsing the United States Mint's online store, but if they choose not to provide PII, they will not be able to make a

purchase online. *Nonregistered Visitors* may decline to provide PII to United States Mint by disabling first-party cookies on their web browser before navigating to the United States Mint online store and refraining from registering and making any purchases in the online store. *Nonregistered Visitors* may also make inquiries by telephone at 1-800-USA-MINT (1-800-872-6468).

Registered Customers may decline to provide PII to the United States Mint, but if they choose not to provide PII, they will not be able to create an online shopping account or enjoy account benefits (such as self-directed one-stop online account and email subscription management, order history access, advance product enrollment, wish lists, and address and credit card storage). They also would not be able to make purchases in the online store. *Registered Customers* may also avoid providing information regarding their browsing habits by disabling first-party cookies on their web browser before navigating to the United States Mint online store, but they will not be able to make any purchases or enjoy *Registered Customer* benefits while first-party cookies are disabled. *Registered Customers* cannot opt out of transactional emails related to a specific order they have placed. *Registered Customers* may cancel their online shopping registration account (or email subscriptions) at any time using their account management tools. *Registered Customers* may also make inquiries by telephone at 1-800-USA-MINT (1-800-872-6468).

Single Transaction Customers may decline to provide PII to the United States Mint, but if they choose not to provide PII, they will not be able to make purchases in the online store. *Single Transaction Customers* may also avoid providing information regarding their browsing habits by disabling first-party cookies on their web browser before navigating to the United States Mint online store, but they will not be able to make any purchases without first enabling first-party cookies. *Single Transaction Customers* cannot opt out of transactional emails related to a specific order they have placed. Single Transaction Customers may also make inquiries by telephone at 1-800-USA-MINT (1-800-872-6468).

Online Assistance Customers may decline to provide PII to the United States Mint, but if they choose not to provide PII, they will not be able to obtain assistance in the online store. *Online Assistance Customers* may also make inquiries by telephone at 1-800-USA-MINT (1-800-872-6468).

Email Subscribers may decline to provide PII to the United States Mint, but if they choose not to provide PII, they will not be able to receive communications from the United States Mint. *Email Subscribers* may also avoid providing information regarding their browsing habits by disabling first-party cookies on their web browser before navigating to the United States Mint online store, but they will not be able to make any purchases or send emails to the United States Mint without first enabling first-party cookies. *Email Subscribers* may unsubscribe from United States Mint communications by contacting Customer Service toll free, 8 a.m. to 12:00 midnight Eastern Time, seven days a week. Within the United States, they may call 1-800-USA-MINT (872-6468), and from outside the United States, call 001-202-898-MINT (6468). Hearing and speech-impaired customers with TTY equipment can reach us at 1-888-321-MINT (6468) Monday through Friday from 8:30 AM to 5:00 PM Eastern Time. They also may write

directly to United States Mint, Customer Service at 4638 E Shelby Drive, Memphis, TN 38118. Subscribers to electronic newsletters *Product and Promotion Updates, Lessons That Make Cents, News Releases, or Coins Online* may unsubscribe by clicking on the "unsubscribe" link on the newsletters received. *Registered Customers* also may unsubscribe from email services online using their account management tools.

Offline Transaction Customers may decline to provide PII to the United States Mint, but if they choose not to provide PII, they will not be able to make purchases offline. If a customer chooses to place an order through a customer service representative via telephone, the customer is notified that the phone call may be recorded for quality assurance and training purposes. Recordation may be avoided by hanging up after hearing this notice (at which point they may opt to order online). If the *Offline Transaction Customer* has previous purchasing history with the United States Mint, that data may be used by the customer service representative to recommend additional (cross-sell) or related higher quality (up-sell) products. The customer has the option to disconnect from the call at any time without providing personal information or placing an order.

Nonregistered Visitors or Customers Who Submit Email may decline to provide PII to the United States Mint, but if they choose not to provide PII, they will not be able to submit email to the United States Mint.

Nonregistered Visitors Who Complete Online Surveys are not required to provide PII to the United States Mint in order to complete a survey. All responses are collected and stored anonymously and are not associated with other account information.

In what ways will individuals be able to indicate their consent to various uses of their information?

Visitors to the online store who do not make any purchases and do not want their browsing information collected (even anonymously) must shut off cookies using the options in their browser before navigating to the online store. The opt-in elections noted (*for Registered Customers, Single Transaction Customers* and *E-mail Subscriber*s) above will be gathered through online forms at various points such as registration and when purchase information is collected at checkout. *Registered Customers* and *Single Transaction Customers* cannot opt out of transactional emails related to a specific order they have placed. Users must opt-in to receive newsletters and marketing/promotional emails; however, for cross-selling purposes, there is no option to opt-out of receiving product recommendations presented to the customer during the browsing session while within the online store. This OMS II functionality provides recommendations based on all customers' past activity on the United States Mint's store website (e.g., browsing and purchasing histories).

Users can manage individual cookie settings on their browsers to ensure data is not collected and stored while they are browsing. However, this will also limit the receipt of cross-selling recommendations in the online store.

D. Attributes of the Data:

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? Why?

OMS II supports the United States Mint's numismatic operations and is intended to provide United States Mint customers with an experience that keeps pace with advancements in both technology and functionality increasingly prevalent in other retail settings. Providing the public with information concerning the United States Mint's numismatic services and products using customer contact information and optional product interest information is one of the principal purposes of OMS II. Processing transactions using customer and recipient information enables numismatic sales and marketing (another one of OMS II's fundamental purposes), along with use of audit trail and employee activity information to allow system management and stability. Certain information requested may also be relevant to future decisions by United States Mint to expand its inventory to sell products related to its numismatic sales mission. Collecting marketing information for this purpose is relevant and necessary to the United States Mint mission.

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

OMS II creates the following new and previously unavailable data about an individual: (1) fraud risk assessments; and (2) data regarding the online browsing activities of customers who opt in to allow tracking of their online activities.

Fraud Risk Assessments: Data are provided by the customer primarily to complete purchase transactions or to enroll in subscriptions. Prior to sending a transaction to Pay.gov for authorization, CyberSource assesses the fraud risk of each web and phone order transaction using a set of business rules and historical data derived from past experiences involving fraudulent transactions. Transactions that exceed the threshold for risk are flagged for manual review by CyberSource staff. The fraud risk assessment provider uses previous transaction information (by any vendor transactions assessed by CyberSource) to match and identify any transactions at potential risk for fraud. CyberSource also tracks and stores the *Registered Customer's* or *Single Transaction Customer's* complete IP address for more accurate transaction matching; however, this information is not stored to identify the owner of the IP address. This information is stored within a historical matching list that tracks shipping and email addresses associated with transactions that met the criteria for high risk of fraud. This information will not be associated with a specific customer account.

Online Browsing Activities: OMS II collects browsing information and aggregates it with visitor IDs (randomly assigned IDs attached to each visitor to the online store) and customer history (for those who opt in) to derive a more sophisticated understanding of United States Mint customers than previously available.

3. Will the new data be placed in the individual's record?

Fraud Risk Assessments: No, this information will not be placed in the individual's record.

Online Browsing Activities: Yes, browsing history of *Registered Customers, Single Transaction Customers* and *Email Subscribers* will be associated with the customer's other information, including his or her email address.

4. Can the system make determinations about employees/public that would not be possible without the new data?

Fraud Risk Assessments: The system does not make determinations about employees or the public. The CyberSource service does not make determinations about employees or the public. Potential fraudulent credit card transactions are flagged using defined business rules and manually reviewed by CyberSource personnel.

Online Browsing Activities: The system does not make determinations about employees or the public. OMS II can allow more sophisticated understanding of the shopping habits of our customers based on analysis of browsing activity in conjunction with past order and subscription habits. OMS II can also create customer groups based on their past activity on the United States Mint's store website, such as purchasing history and product interests, using the new data to create marketing emails specific to the customer groups (this functionality will be enabled once OMS II has sufficient data on customers' past activities and purchasing histories to create this new data); this function would allow customers to be clustered by their purchase behavior on the United States Mint's store website and classified into behavior classes and clusters.

Information regarding the browsing activity of *Registered Customers, Single Transaction Customers* and *Email Subscribers* (i.e., who opt in to allow tracking of their browsing activities) collected on the United States Mint's online store can indicate and track their purchasing habits and interests to optimize overall marketing efforts.

5. How will the new data be verified for relevance and accuracy? Refer to the information provided for question C. 3 above.

Fraud Risk Assessments: Credit card transactions are flagged based on defined business rules. All flagged transactions are reviewed manually by CyberSource personnel, who determine whether to authorize or decline the credit card transaction manually.

Online Browsing Activities: Providing the public with information concerning the United States Mint's numismatic services and products using customer contact information and optional product interest information is one of the principal purposes of OMS II. Collecting marketing information for this purpose is relevant and necessary to the United States Mint mission. Derived/aggregated information is updated daily and regularly reviewed for relevance. Periodic testing and verification occurs to validate the accuracy of the derivation or aggregation procedures.

6. Are the records in the system all maintained for the same purpose? Do the records in this system share the same security requirements?

All records in OMS II share the same overall purpose (numismatic operations) and security requirements. OMS II is categorized as "moderate" for the purposes of potential

impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability) according to Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, and the system and information are secured accordingly. All aspects of OMS II will be subject to the security assessment and authorization process to certify OMS II for authorization to operate. The service provider ensures all applicable security and privacy controls and policies are employed, tested and monitored on a continuous basis as outlined in Treasury Directive 85-01, *Department of the Treasury Information Technology Security Program*.

If the customer chooses to register, online customer account information (name, log-in username, email, physical address and internet protocol address) are maintained to facilitate future transactions (returns and credit) and subscription enrollments. Customers also have the ability to store saved addresses and credit card payment data.

Customer information (including order information), as well as the information regarding browsing behavior during previous visits to the United States Mint's online store (for opt in customers), are used to maintain an accurate profile of the customer to allow the marketing group to personalize communications to the customer, effectively use predictive analytics to develop insights and create marketing programs to leverage those insights, and understand customer purchase behavior patterns to be used for marketing and merchandising on the website.

Transaction data that has Federal financial management implications for collections and revenue must also be maintained to support accounting and audit objectives.

i. Will the records in the system share the same Routine Uses?

All of the records in OMS II will share the same routine uses outlined in the Altered System Notice, Treasury/ United States Mint - .009 – Order Management System (OMS) (*replacing* United States Mint .009, "Retail Sales System").

7. If the <u>data</u> is being consolidated, what safeguards and controls are in place to protect the data from unauthorized access or use?[5]

All United States Mint systems and those operated on behalf of the United States Mint are subject to IT security controls in accordance with Treasury Directive 85-01. This includes an access control policy that is monitored and enforced to ensure that the use of

[5] If the data is being consolidated, that is, combined or united into one system, application, or process, then the existing controls, if any, should remain to protect the data. If needed, strengthen the control(s) to ensure that the data is not accessed inappropriately or by someone unauthorized to access the data. These controls will help to prevent unauthorized use from occurring. Minimum sets of controls are outlined in OMB Circular A-130, Appendix III. Another consideration is the use of Role Based Access Controls (RBAC). For more information on RBAC, see http://csrc.nist.gov/rbac/.

The Treasury Information Technology (IT) Security Program Manual TD P 85-01, describes the practice of identification and authentication (Section 5, page 5-1) that is a technical measure that prevents unauthorized people or processes from accessing data. The IT Security Program Manual (Section 3) outlines the requirement for a system security plan to include the implementation of the technical controls associated with identification and authentication.

United States Mint networks and information systems shall be limited to those persons with authorized access. United States Mint employees, as well as government contractor and subcontractor employees, must follow access control procedures that include an access approval process, unique user IDs, user authentication, password management and immediate removal of access for persons whose access privileges have been suspended or revoked due to a change in employment status. Prior to receiving access to OMS II, users are vetted as part of the employment process and complete IT security awareness and privacy training.

The OMS II service provider is responsible for safeguarding all data and processes in accordance with Federal and Department of the Treasury regulations and as outlined in the terms and conditions of the United States Mint's contract with the OMS II service provider, PFSweb.

If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

The United States Mint implements proper controls in OMS II to protect the data and prevent unauthorized access. All United States Mint systems are subject to access controls in accordance with Treasury Directive 85-01. In addition, the United States Mint has an internal policy that is monitored and enforced to ensure that the use of United States Mint networks and information systems shall be limited to those persons with authorized access. United States Mint managers and system administrators enforce access control procedures that include an access approval process, unique user IDs, user authentication, password management and immediate removal of access for persons whose access privileges have been suspended or revoked due to a change in employment status.

The OMS II service provider is responsible for safeguarding all data and processes in accordance with Federal and Departmental regulations and as outlined in the United States Mint's contract with the OMS II service provider, PFSweb.

8. How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

United States Mint service provider employees and subcontractor employees retrieve customer account data using personal identifiers including name, address, phone, email, order number and log-in name. Credit card information is not accessible to United States Mint employees, service provider employees and subcontractor employees, and cannot be viewed directly. When interacting with a customer's account or orders, the credit card data will be masked and can only be sent for authorization, replaced, or deleted. A credit card number is not used to retrieve any account data.

The fraud risk assessment provider processes order transaction information as it is received, which eliminates the need to retrieve any data using any personal identifiers.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to these reports?

Reports from the customer database can be produced on customer profile information, sales order information, historical data, and statistical data; reports are usually generated based on order and sales information, rather than customer information, for marketing and product sale analyses. Reports containing customer information are necessary when individual customer orders or accounts require research to resolve issues. Reports are only available to United States Mint employees with a need to know the information contained in the reports, or to third parties to the extent required by the Freedom of Information Act or permitted by the Privacy Act, including system routine uses.

If the United States Mint needs access to customer or system data in the event of a security or privacy breach, this information will be obtained through the service provider based on operational need. OMS II security monitoring and audit reports will be provided to the United States Mint on a regular basis (as required by the contract) or, in the case of a system security event or incident, to United States Mint employees with a need to know and otherwise permitted by the Privacy Act.

E. Maintenance and Administrative Controls:

1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

As implemented for the United States Mint, OMS II will be assigned to one of two data centers that will serve as the primary data center. The other data center will serve as the backup.

Replication of production databases and data to backup data centers are performed using automated systems and system checks; automated tools are utilized to ensure the completeness and accuracy of the data replication and integrity. There are automated monitoring systems in place that will alert the service provider and contractor staff of any replication failures. There are standard operating procedures in place to address any failures, as well as for regular monitoring activities.

2. What are the retention periods of the data in this system?

Data removed from OMS II or reports generated from OMS II will be maintained and disposed of in accordance with records retention schedules approved by the Archivist of the United States pursuant to National Archives and Records Administration (NARA) requirements.

Electronic information in OMS II is being evaluated to establish proper maintenance and disposition of records contained in the system and will be maintained in a secured environment until approved disposition is identified in accordance with NARA requirements.

3. ***What are the procedures for disposition of the data at the end of the retention period[6]?***
The service provider and subcontractors will purge records consistent with NARA records retention schedules and contractual requirements, and will provide evidence of purging and destruction to the United States Mint.

4. ***Is the system using technologies in ways not previously employed (e.g., monitoring software, Smart Cards, cookies/tracking, Caller ID, migration of paper records)?***
OMS II's technology is predominantly the same as the previous *eCommerce* system employed by the United States Mint with the following exceptions:

    - While the United States Mint currently uses anonymous analytics and surveys to conduct marketing analysis on customer behavior and website interaction behavior, OMS II will permit more detailed analytics than previously available to the bureau, and will additionally allow analysis of individually identified (non-anonymous) behavior of opt-in customers' past activity on the United States Mint's store website. One of OMS II's applications, AgilOne, collects information at the customer level and calculates dimensions of customer behavior (to include order counts, average order value, lifetime average order value, lifetime order total, order values by state or zip code, and derived gender).
    - OMS II also provides the functionality for "cross-selling" in which product recommendations are made based on aggregated analysis of United States Mint store website purchase behavior of customers—not an individual's purchase history or other information specific to any individual.
    - The point-of-sale portion of OMS II includes six mobile devices (will be used at United States Mint Headquarters and will be available for travel to conferences or other sites). The use of these mobile devices is an addition to the capabilities the United States Mint has today. These devices will be used to process customer information on-the-go.
    - OMS II will use a combination of business rules to assess the potential fraud risk of each credit card transaction.
    - For customers who have registered accounts, the new online store will determine which products to promote to them based on their past order history on the United States Mint's online store.
    - Live chat (customer interactions but customers cannot place orders through this medium).
    - OMS II will allow customer service representatives to take screen captures of information inputted during customer interactions (including order transactions and processing).
    - The SDR stores customer credit card information in a tokenized (credit card information is replaced with random values) and encrypted manner.

5. ***How does the use of this technology affect public/employee privacy?***

[6] Disposing of the data at the end of the retention period is the last phase of life cycle management. Contact the bureau's Records Management Office for further assistance. Records subject to the Privacy Act have special disposal procedures.

All aspects of OMS II will be subject to the security assessment and authorization process to certify OMS II for authorization to operate.

- While OMS II allows a closer and more sophisticated understanding of customer behavior than previously available to the bureau (and will offer users who opt in a customized shopping experience, including personalized suggestions), customers who prefer not to enable this level of personalization can opt out of creating a profile and can further limit the information collected about them by disabling the use of tracking technologies via their web browser settings before they navigate to the United States Mint's online store.
- OMS II also includes remarketing capabilities (the ability to show advertisements to users who previously have visited the United States Mint's website as they browse the Web) based on a Tier 2 cookie (does not collect or store PII). The web browser cookie can track and store user behavior based on the customer's prior browsing history on the United States Mint's store website to provide product suggestions. Users can manage cookie settings to ensure browsing history is not tracked.
- For the mobile elements of OMS II, policies on the use and handling of the devices will be developed or applied, and the devices will be subject to a United States Mint security assessment.
- CyberSource will use business rules with which the United States Mint has agreed to identify potentially fraudulent credit card transactions. Once those transactions have been identified, CyberSource personnel (not the system) make the determination to authorize or decline the transaction.
- For customers with registered accounts, the new online store determines which products to offer them based on past United States Mint order history.
- Policies exist regarding secure storage of the live chat (consisting of customer interactions but not orders) and email correspondence. Specific guidance is being provided to customer care representatives on types of information appropriate to store in these formats so they discourage customers from providing it.
- The SDR stores customer credit card information for active orders in a tokenized and encrypted manner. The new technology implemented for the SDR does not affect public or employee privacy; the tokenized and encrypted data has an additional layer of security to prevent any potential breaches.

6. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

OMS II has the capability to identify and locate individuals for verification of orders and to market future events and products, but it does not monitor individuals outside of their activity on the United States Mint's online store.

OMS II also monitors the audit logs of employees, government contractors and subcontractors to ensure proper use of the information in OMS II.

7. What kinds of information are collected as a function of the monitoring of individuals?

In addition to collecting information on browsing activity as noted above, audit logs are collected for all activity associated with OMS II's usage (including invalid logon

attempts and access to data in accordance with Treasury Directive 85-01 which requires technical access and audit controls). Access is monitored for United States Mint employees, as well as government contractor and subcontractor employees (including service-providers) alike.

8. What controls will be used to prevent unauthorized monitoring?

OMS II is monitored for unauthorized use through automated audit logging. All system users and user activity within OMS II is tracked and recorded; system administrators with approved privileges and a need-to-know have read-only access to review system audit logs.

9. If the system is web-based, does it contemplate use of persistent cookies or other tracking devices?

OMS II uses the following types of persistent cookies, and their respective tiers, as defined by OMB Memorandum M-10-22:

OMS II employs web measurement and customization technologies (to include Tier 2 and Tier 3 web measurement and customization technologies) to track customer information in order to customize the online store browsing experience. Based on the collected information, the United States Mint will conduct marketing analysis in order to offer numismatic products and services to the public in the most effective and efficient manner.

When browser cookies are enabled, *Nonregistered Visitors* browsing the United States Mint online store are assigned an auto-generated visitor identifier to track browsing behavior, IP address (limited to the broad geo-location based on first six digits of IP address) and device settings. The full IP address is collected for *Registered Customers*. The information is used to improve the online store based on behavioral analysis (products viewed, pages browsed, previous order history and purchasing habits) and is not associated with any PII. This Tier 2 web measurement and customization technology can be disabled by navigating to the internet browser setting and disabling cookies.

When browser cookies are disabled, visitors browsing the United States Mint online store are not tracked at the individual level (i.e., they cannot be identified individually); all tracking information is aggregated and considered "anonymous." This information includes online store browsing behavior, device settings and general geo-location based on truncated IP address.

If a customer *(Single Transaction or Registered)* signs up for newsletter subscriptions or purchases products when logged in as a guest (i.e., a *Single Transaction Customer*), PII is provided by the customer to complete a transaction. A Tier 3 cookie will associate online store browsing behavior with the customer account using the email address provided.

Customers have the option to register for an online store account by explicitly consenting (opting-in) to the United States Mint's collection and storage of PII (name, address, phone number, email address and credit card information).

i. If so, has a memorandum been prepared that documents the tier analysis and classification of the cookies/devices under OMB Memorandum M-10-22?
Yes.

ii. If the answer to 9.i is yes, please provide a copy of the memorandum to the Office of Information Security and forward separately with this PIA when circulating the PIA for review. If no, such a memorandum must be prepared and approved by the Director before implementation and before any necessary Tier 3 permission can be sought.
See answer to 9i above.

iii. If a tier analysis has been performed and documentation prepared, are any of the cookies or other tracking devices classified as Tier 3?
Yes. A tier analysis has been performed and provided to the United States Mint CIO. There are multiple aspects of OMS II that have been classified as Tier 3. That analysis has been attached to this Privacy Impact Assessment.

iv. If the answer to iii above is yes, has official written permission from Treasury Office of the CIO been obtained as required by OMB Memorandum M-10-22?
OMB Memo M-10-22 documentation is being finalized and routed to appropriate approvers.

*10. If the system is being modified, will the Privacy Act System of Records Notice require amendment or revision? **Explain.***
The existing SORN was updated. Treasury/ United States Mint - .009 – Order Management System (OMS) replaced United States Mint .009, "Retail Sales System."

F. Access to Data:

1. Who will have access to the data in the system? (e.g., users, managers, contractors, others) Will those with access to the data have appropriate training and security clearances to handle the sensitivity of the information?
Access to PII in OMS II is limited to United States Mint personnel, government contractor personnel, and subcontractor personnel. Authorization to access this PII is determined by the business function to be performed by the user accessing the information and, in part, by the nature of the information being accessed.

A range of United States Mint personnel and contractor personnel are expected to have access to some or all of the system data. Such personnel can include United States Mint IT employees; account and program managers; call center staff; credit/financial staff; accounting personnel; distribution center staff; and persons involved in responding to order history or other inquiries concerning customer interactions or system functions received from customers or third parties as permitted under the Privacy Act (including system routine uses) and other applicable law.

All users with access to a United States Mint system and/or systems operated on the behalf of the United States Mint are required to successfully complete information security and privacy training. Personnel with access to United States Mint systems and networks must be vetted through a United States Mint security clearance process prior to receiving access. Those provided with access to the system and the data receive access based on access control standards that restrict any user's level of access to the least amount required to accomplish assigned duties. In providing this access, role-based least-access principles are used to enforce the segregation of duties. All users are assigned to a user class/group, and access to data, programs and files is allowed or restricted based on that role. User groups and access are reviewed on a regular basis for stale or inactive accounts.

2. ***How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?***
Access to OMS II data (including PII) by United States Mint employees, government contractors, and subcontractors is determined by the business function to be performed by the user accessing the information and, in part, by the nature of the information being accessed.

United States Mint employees, government contractor employees, subcontractor employees, and system administrators enforce access control procedures that include an access approval process, unique user IDs, user authentication, password management and immediate removal of access for persons whose access privileges have been suspended or revoked due to a change in employment status.

Further, access to data by administrative users (both contractor staff and United States Mint employees) is provided in accordance with the United States Mint Information Security Policy. This information systems access policy establishes procedures for access control of all United States Mint IT systems in accordance with Treasury Directive 85-01. This policy has been made available or distributed to appropriate personnel.

United States Mint employees, government contractor employees, subcontractor employees, and system administrators enforce access control procedures that include an access approval process, unique User IDs, user authentication, password management and immediate removal of access for persons whose access privileges have been suspended or revoked due to a change in employment status. Furthermore, a monthly audit is conducted to determine if the access granted is still needed.

Access to information and data is restricted to authorized personnel on a "need-to-know" basis, with contractor employees and United States Mint personnel having greater or lesser access to information in the database depending on their duties.

Registered customers may access registration information and order history online with their valid access credentials. United States Mint Privacy Act regulations at 31 C.F.R. § 1.26, et seq., and Appendix H to Part 1, subpart C, provide the process for an individual to request access to Privacy Act records on that individual contained in United States Mint systems of record.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

All United States Mint employee and contractor user access is restricted based on access control standards that restrict the level of access to the least amount required to accomplish assigned duties.

Registered customers may access registration information and order history online with their valid access credentials. United States Mint Privacy Act regulations at 31 C.F.R. § 1.26, et seq., and Appendix H to Part 1, subpart C, provide the process for an individual to request access to Privacy Act records on that individual contained in United States Mint systems of record.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

The entire OMS II will be authorized in accordance with Treasury Directive 85-01 at the "moderate level" for the purposes of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability) according to Federal Information Processing Standards Publication 199.

United States Mint employee and contractor employee access is restricted based on access control standards that restrict their respective levels of access to the least amount required to accomplish assigned duties. Further, all such employees are required to complete security and privacy awareness training and sign the IT System User Rules of Behavior which outline the appropriate and mandatory behavior of all those using United States Mint's IT systems or systems operated on behalf of the United States Mint.

Logical security is used to restrict access to the least amount required to accomplish assigned duties. Employee and contractor access is logged and reviewed on a regular basis. Encryption restricts access to credit card information in the SDR.

The United States Mint will perform periodic audits and security reassessments of the OMS II to confirm compliance. The contractor is obligated to monitor and notify the United States Mint of the ongoing security status of OMS II.

5. Are contractors involved in the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

OMS II is a turn-key system developed, provided and maintained by a contractor. As part of the service provided, the contractor also offers customization to the provided services in accordance with its contract with the United States Mint. Privacy Act contract clauses and other regulatory compliance obligation measures were included in the contractor's contract with the United States Mint. In addition, all United States Mint IT-related contracts are subject to information security reviews during the procurement process.

6. ***Do other systems share data or have access to the data in this system? If yes, explain.***
   Other systems will not share data or have access to the information contained in OMS II, except as specifically shared via interfaces as described in other sections of this Privacy Impact Assessment.

7. ***Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?***
   The United States Mint's CIO is ultimately responsible for protecting the privacy rights of the public and employees affected by OMS II. The CIO ensures that OMS II has all security and privacy controls in place and properly operating to prevent breach of PII. The service provider and all users with access to OMS II and its data are also required to follow policies and procedures that protect the privacy rights of the public and the employees.

8. ***Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If yes, explain.***
   Other agencies will not have access to the information contained in OMS II, except as specifically shared via interfaces as described in other sections of this Privacy Impact Assessment.

9. ***How will data be used by the other agency(s)?***
   Not applicable.

10. ***Who is responsible for assuring proper use of the data?***
    The United States Mint's Associate Director of Sales and Marketing is ultimately responsible for assuring proper use of the data. The service provider and all users with access to OMS II and its data are also required to follow policies and procedures that assure proper use of the data.