Sales Automation System (SASy)

Privacy Impact Assessment

3 April 2020

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. It requires GSA to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The template also accords with 1878.2A CIO P - Conducting Privacy Impact Assessments; is designed to align with GSA businesses processes; and can cover all of the systems, applications or projects logically necessary to conduct that business.

The document is designed to guide GSA program managers, system owners, system managers and developers as they assess potential privacy risks during the early stages of development and throughout the system, application or project's life cycle.

The completed PIA shows how GSA ensures that privacy protections are built into technology from the start, not after the fact when they can be far more costly or could affect the viability of performing GSA's work. Completed PIAs are available to the public at gsa.gov/privacy (https://www.gsa.gov/portal/content/102237).

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. For example:

This document contains important details about *[system, application or project name]*. *[GSA office]* may, in the course of *[program name]*, collect personally identifiable information ("PII") about the people who use such products and services.

An example of a completed PIA is available at: https://www.gsa.gov/portal/getMediaData?mediaId=167954

Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.

Stakeholders

Name & Email of Information System Security Manager (ISSM):

- Jonathan Wallick

Name & Email of Program Manager/System Owner:

- Narendra Rao

Signature Page

Signed:

DocuSigned by:

Jonathan Wallick

51A2B47547C34D9...

Information System Security Manager (ISSM)

DocuSigned by:

Narendra Rao

776FE828D4EF405...

Program Manager/System Owner

DocuSigned by:

Richard Speidel

171D5411183F40A...

Chief Privacy Officer. Under the direction of the Senior Agency Official for Privacy (SAOP), the Chief Privacy Officer is responsible for making sure the PIA contains complete privacy related information.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third party-services and robotics process automation (RPA).	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed CPO email address	2.3
11/28/2018	Added new stakeholders section to streamline process when seeking signatures & specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4

Table of contents

4.2 Will GSA share any of the information with other individuals , Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

4.4 Will the system, application or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about the Sales Automation System (SASy). GSA Office of Personal Property Managment may, in the course of Property Sales, collect personally identifiable information ("PII") about the people who use such products and services. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles ("FIPPs"), a set of eight precepts that are codified in the Privacy Act of 1974.[2]

System, Application or Project

Sales Automation System (SASy)

System, application or project includes information about

GSA employees and contractors, Federal agency employees and contractors, company and public users (domestic and international).

System, application or project includes

- Name and date of birth
- Contact Information (addresses, telephone numbers, and email address)
- Social Security Number, TIN or other government-issued identifiers
- Financial Information (credit card numbers and expiration dates)
- Information about individuals provided by third parties (accept or refer decision from Experian PreciseID identity proofing service)

Overview

SASy FISMA System

The Sales Automation System (SASy) system is a Major Application (MA) that resides on a Unisys ClearPath mainframe platform. As defined in OMB Circular No. A-130 -

Security of Federal Automation Information Resources, Appendix III, Major Application (MA) requires "... special management attention due to the risk and magnitude of harm that could occur."

The SASy system is comprised of several sub-applications that support the sale and auction of surplus federal personal property and real estate as well as the reverse auctioning of government commodities and services. The five sub-applications that comprise the SASy system are:

- Sales Automation System (SASy) sub-application, (Note: SASy sub-application is used to differentiate the main system name from the sub-application name)
- GSAAuctions, which contains approximately 400,000 PII records;
- MySales, which contains approximately 422,000 PII records;
- ePay, which contains approximately 2,000 PII records; and
- ReverseAuctions.

The SASy FISMA system supports the following business stakeholders in the sale of surplus property and real estate:

- GSA FAS GSS Office of Personal Property Management Division who is responsible for the disposal, by sale, of all government owned personal property reported to GSA.
- Department of Interior (DOI) Aviation Management Directorate (AMD) in the sale of Aircraft and Aircraft Parts.
- GSA PBS Real Property Division in the sale of surplus federal land and buildings.
- GSA FAS Office of Fleet Management for the sale and payment of surplus Fleet vehicles.

The SASy FISMA system also supports the following business stakeholders in the reverse auctioning of commodities and simple services:

- GSA GSS OMS FSSI OS3 Orders

SASy sub-Application

The Sales Automation System (SASy) sub-application is a Unisys ClearPath ePortal web application that is used to process the receipt and sale of surplus government property in an efficient, expeditious manner and obtain maximum net returns with a minimum of inconvenience to holding agencies. The SASy sub-application supports GSA regulations pertaining to excess/surplus property utilization and disposal for the ten GSA FAS domestic regional agencies. Property is entered directly into SASy or received from the GSAXcess system. SASy includes property not successfully transferred within the Federal Government (GSAXcess) and other eligible organization's property that does not qualify for reutilization or donation. SASy provides automated inventory control of this surplus in support of GSA's mission to provide the most efficient and cost-effective method for Federal Agencies to use and dispose of personal property.

SASy Regions are able to: review items that are available for sale, create sales and property lots for the different methods of sale, and post and maintain awards and payments for audit purposes. SASy helps GSA regional offices by automating the following functions: Managing inventory of personal property for sale, creating property lots for sale, handling sales offerings, maintaining bidder information, awarding and administering sales contracts, processing payments, informing customer agencies about the status of their property, maintenance of bidders and defaulted bidders, maintains performance metrics used to determine whether or not planned operational objectives and goals are being met, and producing reports.

The SASy sub-application electronically interfaces with the following GSA internal systems: ePay, GSAAuctions, GSAXcess, GSA Ancillary Financial Applications (GSA AFA), GovSales, WebARM, FMS - Fleet Management System, reportsportal.fas.gsa.gov, SASy JReport Dashboard.

The SASy sub-application electronically interfaces with the following external systems: NASA Integrated Asset Management.

SASy Sub-Application PII and PCI DSS

Specific information about individuals that is collected, generated or retained

These PII and PCI DSS elements are collected at the time of bidder account creation and payment for individuals that register, bid, and pay for surplus property sold on GSAAuctions or via other sale methods and elect to pay online in person, or over the phone and are stored in the SASy database.

- First and Last Name
- Home address
- Email address
- Telephone number
- Social Security Number or Tax Identification Number

- Credit card number (PCI DSS)
- Expiration date (PCI DSS)

Securing Sensitive PII and PCI Data

Data is secured during transport via HTTPS TLS 1.2, RSA key exchange, and AES_256_GCM cipher. Data secured at rest is comprised of:

- SSNs and Primary Account Numbers (PANs) are key-encrypted with AES256 using the cryptographic libraries on the Crypto common appliance (based on the Microsoft Crypto SDK) and stored in the SASy database.
- Disk encryption is used in addition to the column-level data key encryption using EMC SAN disk encryption.

Note: Primary Account Number (PAN) is specific to PCI DSS. PAN IS a key piece of cardholder data that a business is obligated to protect under the PCI DSS compliance.

Use of Social Security Numbers

The primary reason that SSNs are required from users is to protect against defaulting bidders. The SSN is used to ensure that when a bidder is in default that they cannot continue to do business with the application until their SSN / account has been removed from default. GSA's legal authority for the collection of SSNs is: Public Law 104-134, Section 21001, The Debt Collection Improvement Act of 1996. The Tax Identification Number (TIN) must be provided by anyone conducting business with the Federal Government from which a debt to the Government may arise. Registration will not be considered if the TIN is not provided. A TIN is defined as an individual's Social Security Number (SSN) or a business entity's Employer Identification Number (EIN).

PII Sharing with GSA systems

The Sales Automation System (SASy) sub-application connects to the GSA Fleet Management System (FMS) and receives bidder name and payment data from FMS for payments made on fleet vehicle sale contracts via a secure database connection.

PII Sharing with external systems

The SASy Sub-Application system does not share PII with external systems.

MySales Application

MySales (MS): MySales is a Unisys ClearPath WEBPCM web application that provides Federal Agencies with the ability to manage their personal property inventory. MySales allows Federal Agencies to report on and manage their surplus, exchange/sale, and forfeited property that has been reported to the General Services Administration (GSA) to sell. It also provides agency custodians and property managers with the ability to check on the status of their property that has transitioned into the GSA Sales Program and withdraw such property because it is no longer available for sale (destroyed/broken, stolen, misplaced, or transfer or donation request). MySales also provides GSA Fleet contracted auctions house users with the ability to select GSA Fleet Vehicles for sale on GSA Auctions. GSA Fleet Auction House Users can select vehicles for sale, send to GSA Auctions, and update sale information.

The MySales electronically interfaces with the following GSA internal systems: SASy sub-application, GSAAuctions, and AutoAuctions.

MySales PII

Specific information about individuals that is collected, generated or retained

These PII elements are collected at the time of registration or account creation from individuals that post vehicles for online auctions and for Federal agency users that require visibility into the status of property being sold by GSA.

- First and Last Name
- Work/Home address
- Email address
- Telephone number

Securing PII Data

Data is secured during transport via HTTPS TLS 1.2, RSA key exchange, and AES_256_GCM cipher. Data is secured at rest by: Disk encryption is used in addition to the column-level data key encryption using EMC SAN disk encryption.

PII Sharing with GSA systems

The MySales system does not share PII with other GSA systems.

PII Sharing with external systems

The MySales system does not share PII with external systems.

ePay Application

ePay is a Unisys ClearPath WEBPCM web application that provides credit card payment transmission and processing functionality for GSA Fleet vehicles sold at auction. The GSA Office of Fleet Management contracts with vehicle auction houses to auction GSA Fleet vehicles. The ePay web application enables auction houses users and successful bidders to process credit card payments for auctions conducted at the auction house. The ePay web application provides the following functionality: credit card payment processing using the ePay web interface and the Pay.Gov OCI interface, download sale information to WebARM via a file interface, update sale and contract information in SASy via a database link, manage user accounts, and configure user roles and security for GSAIT, GSA Property and Fleet Users via the web interface.

The ePay application electronically interfaces with the following GSA internal systems: SASy and WebARM. **Note**: WebARM and FMS relate in the same way as SASy and ePay.

The ePay application electronically interfaces with the following external systems: Pay.Gov.

ePay PII and PCI DSS

Specific information about individuals that is collected, generated or retained

These PII and PCI DSS elements are collected at the time of payment from individuals that purchase vehicles at a GSA Fleet vehicle auction and are stored in the ePay database.

- First and Last Name
- Home address
- Email address
- Telephone number
- Credit card number (PCI DSS)
- Expiration date (PCI DSS)

Securing Sensitive PII and PCI Data

Data is secured during transport via HTTPS TLS 1.2, RSA key exchange, and AES_256_GCM cipher. PII Data is secured at rest by: PANs are Key encrypted AES256 using the cryptographic libraries on the Crypto common appliance (based on the Microsoft Crypto SDK) and stored in SASy database. Disk encryption is used in addition to the column-level data key encryption using EMC SAN disk encryption.

PII Sharing with GSA systems

The ePay sub-application connects to the GSA Fleet Management System (FMS). The FMS system receives bidder names and addresses from ePay for payments made on GSA Fleet vehicles via a secure database connection.

PII Sharing with external systems

The ePay sub-application connects to the Treasury Pay.Gov service via a secure HTTPS interface for electronic payment. ePay shares Name, Address, Credit Card Number for Treasury Pay.Gov. The ePay - Treasury Pay.Gov connection has the following agreement in place: Treasury Agency Configuration Template (ACT), Signed 8/23/2004.

GSAAuctions Application

GSAAuctions is a Unisys ClearPath WEBPCM web application that offers the general public the opportunity to bid on a wide array of Federal assets. GSA Auctions offers Federal personal property and real estate assets ranging from commonplace items (such as office equipment and furniture) to more select products like scientific equipment, heavy machinery, airplanes, vessels, vehicles, residential and commercial real estate. The auctions are web based or live events. Web auctions allow all registered participants to bid on items within specified timeframes. Live auction listings display information about the asset including where and when the auction will be conducted. Bidders may register, browse and search for items, bid on items and pay for items that they have won using Pay.Gov's OCI interface.

During registration, bidders can optionally supply a credit card PAN that is used by Experian to aid in identity verification. The GSA Auctions administrator interface is used by agency users to create and manage auctions and by system and account admins to perform auction and user account management functions. GSA Public Building Service (PBS) can create and manage real estate auctions. Department of Interior can create and manage aircraft auctions. GSA Office of Personal Property Management (OPPM) can manage auctions and user accounts. The GSA FAS OPPM / Fleet auctions are created in the Sales Automation System (SASy) and MySales (for GSA Fleet remarketing) applications and are sent to GSAAuctions for bidding, award and payment. GSAAuctions receives sale and bidder default information from the SASy application. Once the bidding process is complete, GSAAuctions sends the winner bid and payment information back to the SASy sub-application for contract completion. If a bidder does not retrieve the property or submit full payment, the bidder is defaulted.

The GSAAuctions application provides these major end user capabilities: user registration, bidder profile updates, bidding, location and distance based search, text and metadata search of open and closed auctions, auction navigation and browsing, social media plugins, email and system notifications, and credit card authorization and charge transactions via Pay.Gov.

The GSAAuctions application provides these major administrator capabilities: auction creation and update capabilities for GSA PBS and DOI AMD users, user and administrator account security functions, auction search, auction cancellation, auction extension, auction bid history and bid cancellation.
The GSAAuctions application electronically interfaces with the following GSA internal systems: SASy sub-application, MySales, GSAXcess, GovSales, ePay, AutoAuctions, JUpload, and SASy JReport Dashboard.

The GSAAuctions application electronically interfaces with the following external systems: Experian PreciseID, Experian BizID, Pay.Gov, and Granicus.

GSAAuctions PII and PCI DSS

Specific information about individuals that is collected, generated or retained

These PII and PCI DSS elements are collected at the time of registration and payment from individuals that register, bid, and pay for surplus property sold on GSAAuctions and are stored in the GSAAuctions database.

- First and Last Name
- Home address
- Email address
- Telephone number
- Date of birth
- Social Security Number or Tax Identification Number
- Credit card number (PCI DSS)
- Expiration date (PCI DSS)
- IP Address

Securing Sensitive PII and PCI Data

Data is secured during transport via HTTPS TLS 1.2, RSA key exchange, and AES_256_GCM cipher. Data is secured at rest by: SSNs and PANs are Key encrypted AES256 using the cryptographic libraries on the Crypto common appliance (based on the Microsoft Crypto SDK) and stored in SASy database. Disk encryption is used in addition to the column-level data key encryption using EMC SAN disk encryption.

Use of Social Security Numbers

A user's SSN is sent to the Experian PreciseID service for identity proofing / verification during account creation. The SSN is used to prevent users from bidding if that SSN is defaulted in SASy or GSAAuctions. The SSN is used to prevent users from registering more than one account with the same SSN. Legal authority for the collection of SSNs in accordance with Public Law 104-134, Section 21001, The Debt Collection Improvement Act of 1996. The Tax Identification Number (TIN) must be provided by anyone conducting business with the Federal Government from which a debt to the Government may arise. Registration will not be considered if a TIN is not provided. A TIN is defined as an individual's Social Security Number (SSN) or a business entity's Employer Identification Number (EIN).

PII Sharing with GSA systems

The GSAAuctions system does not share PII with other GSA systems.

PII and PCI Sharing with external systems

The GSAAuctions sub-application connects to Experian's PreciseID service via a secure web service for Identity authentication. GSAAuctions shares Name, Address, Date of Birth, SSN, Phone, and Credit Card Number (optional) with Experian. The GSAAuctions - Experian PreciseID connection has the following agreement in place: Experian Data Use Addendum (DUA), Signed 3/23/2017. SASy does not share any information with Department of Interior (DOI) systems.

The GSAAuctions sub-application connects to Treasury Pay.Gov service via a secure HTTPS interface for electronic payment. GSAAuctions shares Name, Address, Credit Card Number for Treasury Pay.Gov. The GSAAuctions - Treasury Pay.Gov connection has the following agreement in place: Treasury Agency Configuration Template (ACT), Signed 8/23/2004.

ReverseAuctions Application

ReverseAuctions is a Unisys ClearPath WEBPCM web application that provides a government managed platform for federal and state and local clients to maximize cost savings on non-complex commodities and simple services. ReverseAuctions solicits vendor bids for various acquisition services contracts, and provides a forum for multiple sellers trying to underbid competitors to meet a specific agency buyer's need. An award can be made to the apparent low bidder if it meets the solicitation terms and conditions and is technically acceptable. ReverseAuctions provides buyers with the ability to conduct reverse auctions and vendors with the ability participate in Reverse Auctions utilizing Blanket Purchase Agreements (BPA), GSA Schedules, set-asides, open market and other available contract vehicles and procedures. ReverseAuctions provides the following functionality to Buyers: authentication, create auctions, update auctions, cancel auctions, upload attachments, award auctions, delegate auctions, receive email notifications and system messages, and create/view reports. ReverseAuctions provides the following functionality to Vendors: authentication, registration, browse and view auctions and auction line items, view awards, upload documents, receive email notifications and system messages, and place and update bids.

The ReverseAuctions application electronically interfaces with the following GSA internal systems: eBuy (buyer authentication), Enterprise Service Oriented Architecture (eSOA), Order Management System (OMS), ReverseAuctions JReport Dashboard, and System for Award Management (SAM).

ReverseAuctions PII and PCI DSS

Specific information about individuals that is collected, generated or retained

These PII elements are collected at the time of registration from companies (potentially individuals) that register and bid on procurements on ReverseAuctions and are stored in the ReverseAuctions database.

- First and Last Name
- Business / Home address
- Email address
- Telephone number

Securing PII Data

Data is secured during transport via HTTPS TLS 1.2, RSA key exchange, and AES_256_GCM cipher. Data is secured at rest by: Disk encryption is used in addition to the column-level data key encryption using EMC SAN disk encryption.

PII Sharing with GSA systems

The ReverseAuctions system does not share PII with other GSA systems.

PII Sharing with external systems

The ReverseAuctions system does not share PII with external systems.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

SASy Sub-Application: The PII and PCI DSS elements are collected at the time of bidder account creation and payment for individuals that register, bid, and pay for surplus property sold on GSAAuctions or via other sale methods and elect to pay online in person, or over the phone and are stored in the SASy database. User PII collection is necessary to process payments, palace an individual in default and to reduce fraud by validating user identity.

MySales: The PII elements are collected at the time of registration or account creation from individuals that post vehicles for online auctions and for Federal agency users that require visibility into the status of property being sold by GSA. User PII collection is necessary to validate user identity and provide the correct system access to users.

ePay: The PII and PCI DSS elements are collected at the time of payment from individuals that purchase vehicles at a GSA Fleet vehicle auction and are stored in the ePay database. User PII collection is necessary to process electronic payments and provide a receipt.

GSAAuctions: The PII and PCI DSS elements are collected at the time of registration and payment from individuals that register, bid, and pay for surplus property sold on GSAAuctions and are stored in the GSAAuctions database. User PII collection is necessary to validate user identity and provide the correct system access to users.

ReverseAuctions: The PII elements are collected at the time of account creation for companies (potentially individuals) that bid on OMS procurements on ReverseAuctions and are stored in the ReverseAuctions database. User PII collection is necessary to validate user identity and provide the correct system access to users.

1.2 What legal authority and/or agreements allow GSA to collect the information?

The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies

1.3 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?

Yes, information in the system can be searched by name, email, DOB, address, DOB, and IP Address. The system title for SORN is Personal Property Sales Program (SASy) (GSA

Auctions). The SORN is available at https://www.gsa.gov/reference/gsa-privacy-program/system-of-records-notices-sorns-privacy-act.

1.4. Has any information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

Not applicable.

1.5. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

A SASy FISMA system retention schedule does not exist in NARA. The record retention schedule is based on retention requirements (1) Debt Collection Improvement Act of 1996. (2) FAR Subpart 4.8—Government Contract Files and (3) FAS 4011 P_1_ SALE HANDBOOK. The retention period applies to all SASy sub-applications.

1. Debt Collection Improvement Act of 1996 — The Office of Personal Property has a data retention need for 7 years. In addition, the following items are archived forever: Hazardous, Aircraft & Aircraft Parts, Vessels and items with contracts over $3 million. The data is retained on disk for at least 7 years. The information is retained in order to satisfy debt collection requirements for non-payment or non-removal of goods per the Debt Collection Improvement Act of 1996. Certain datasets have never been purged. The retention applies to data on disk, but not to tape backups.
2. FAR Subpart 4.8—Government Contract Files stipulates retention requirements in section 4.805 Storage, handling, and contract files that "Contracts (and related records or documents, including successful and unsuccessful proposals, except see paragraph (c)(2) of this section regarding contractor payrolls submitted under construction contracts)" have a retention period of "6 years after final payment."
3. The FAS 4011 P_1_ SALE HANDBOOK specifies specific retention requirements for sale contract files in "CHAPTER 7. SALES/CONTRACT FILES." Section 3 states: Retention (GSA ADM). Office sales/contract files containing contracts of $25,000 or less must be maintained by the regional office or sub-office for 6 years after final payment and then destroyed. Files containing any individual contract(s) of $25,000 or more must be held locally for 2 years after

final payment and then retired to the Federal Records Center for retention for 4 years.

a. Aircraft Files -- Shall be retained indefinitely.
b. Sales over $3 Million-- Shall be retained indefinitely.
c. Hazardous Material Files Sales/contract files covering the sale of hazardous material must be retained at the regional office for 3 years and at the Federal Records Center for 7 years. This is required to identify purchasers who dispose of hazardous material in an unlawful manner."

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

The purpose of collection of PII is specified at the time of collection. The PII and PCI DSS information collected are used only for the intended purposes for identity proofing, electronic payment, and debt collection.

Privacy Risk: Unauthorized access. A SASy system user may have access or gain access to PII that is not required by their job role. SASy administrators are authorized by the business line and the branch manager with necessary permissions to view, create, update and delete user data. Users with elevate privileges require a user access request form that indicates the roles required and is signed by the account group owner.

Mitigation: Annual User certification is conducted to ensure that:

1. The user account is still active,
2. All privileged users have a signed access request form,
3. Only Roles Necessary for that individual's job function are granted,
4. Roles Restricted to least privileges necessary to perform the individuals job responsibilities, and
5. Privileges assigned are based on the individual's job classification and function.

Privacy Risk: Data leakage. Sensitive PII and PCI Data is stored in the GSAAuctions, ePay and SASy Databases. If the appropriate controls are not in place then data could be leaked externally.

Mitigation: Data is secured during transport via HTTPS TLS 1.2, RSA key exchange, and AES_256_GCM cipher. PII Data is secured at rest by: PANs are Key encrypted AES256 using the cryptographic libraries on the Crypto common appliance (based on the Microsoft Crypto SDK) and stored in SASy database. Disk encryption is used in addition to the column-level data key encryption using EMC SAN disk encryption.

Privacy Risk: Web site vulnerabilities. User PII or PCI DSS information could be compromised if the system or it's sub systems have exploitable vulnerabilities.

Mitigation: Monthly Netsparker web application scans, and biweekly host scans are conducted and the results are communicated to the application and hosting team team for resolution. Additionally penetration tests are conducted in the event of a suspected incident or during the A&A process. All application related findings regardless of source are tracked in the SASy/Auctions Jira project and remediated according to their priority / impact (critical, high, medium, low). Environment related findings are tracked and mitigated by the Unisys hosting team in service now.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

GSAAuctions users are notified during the "GSAAuctions Terms & Conditions review and acceptance" registration process step of what data will be collected and retained. This information is discussed at length on the Bidder Information and Registration tab of the Terms and Conditions. The terms and conditions are provided to the user for review and acceptance after a username and password are created and prior to data collection. Additionally there is a secondary terms and conditions notice that relates specifically to the Experian PreciseID and BizId identity proofing requirements. This Fair Credit

Reporting Act (FCRA) notice is also reviewed and accepted by the user prior to data collection and retention.

ReverseAuctions – General Terms and Conditions are posted on the website regarding open market vendor registration process.

SASy, ePay & MySales – There are no terms and conditions listed on the website. User accounts are created upon request to conduct certain job duties.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

There are no documented SASy system risks that relate to openness or transparency.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system, application or project?

GSA employees, GSA Contractors, Federal agency employees, Company users, Individual/Public users (this includes US and Non-US residents and international users).

3.2 What PII will the system, application or project include?

The following information is collected by each sub-application:

Sales Automation System (SASy) – Collects following information from Individual and Company bidders/users who are awarded a sales contract

- First and Last Name
- Home address
- Email address
- Telephone number
- Social Security Number or Tax Identification Number
- Credit card number

GSAAuctions - Collects following information from Individual and Company bidders/users. Individual and Company users self-register in the application.

- First and Last Name
- Home address
- Email address
- Telephone number
- Date of birth
- Social Security Number or Tax Identification Number
- Credit card number
- IP Address

ePay – Captures the following information during payment process

- First and Last Name
- Home address
- Email address
- Telephone number
- Credit card number

MySales – Collects following information during account creation

- First and Last Name
- Home address
- Email address
- Telephone number

ReverseAuctions – Maintains following information. One set of Vendor users self-register in the application.

- First and Last Name
- Business / Home address
- Email address
- Telephone number

Additional information gathered from individuals: International bidders registering on GSAAuctions and failed bidders attempting registration on GSAAuctions are asked to provide 2 forms of identification for identity verification to registration@gsa.gov. The Office of Personal Property Central Office staff verifies the documents sent by bidders. Once the documents are verified the central office uses the GSAAuctions Application – Administrator interface to override international and failed users so as to complete registration. Once the users are registered, the central office staff deletes the emails containing identity documents. Some bidders mail personal identity documents to the Office of Personal Property. The documents are shredded after verification.

GSAAuctions uses past bidding history data based on product categories to identify target users to send marketing emails for upcoming sales. The bidders are selected by random (50% sampling) where marketing emails are sent on a daily basis. No bidding history to date has been purged.

The GSAAuctions sub-application uses Experian products (PreciseId for Individual user and BizID for Company users) to get a decision (Accept or Refer). The application uses this decision to make a decision on approving users as registered bidders. For Experian service PreciseId, GSAAuctions sends Individual SSN, name, address and optionally credit card number to get a decision. For Experian service BizId, GSAAuctions sends Company TIN, company name and address to get a decision. The results of the "Accept or Refer" decision are saved in GSAAuctions.

ReverseAuctions – Only FSSI vendors that are allowed to bid on OMS orders can currently access the ReverseAuctions system. Their accounts are created by system admins.

3.3 Why is the collection and use of the PII necessary to the system, application or project?

GSAAuctions Identity proofing – The GSAAuctions sub-application uses Experian products (PreciseId for Individual user and BizID for Company users) to get a decision (Accept or Refer). The application uses this decision to make a decision on approving users as registered bidders. For the Experian service PreciseId, GSAAuctions sends Individual SSN, name, address and optionally credit card number to get a decision. For the Experian service BizId, GSAAuctions sends Company TIN, company name and address to get a decision. The results are saved in GSAAuctions. GSAAuctions also holds credit card payment information for all payments made for awarded auctions. Other non-PII data will not be useful for identity proofing as well as collecting credit card payment.

SASy – SASy stores bidder information for all sales conducted by the Office of Personal Property and Fleet. This information is needed to process payments, handle disputes, and process defaults for non-payment and non-removal.

ePay – ePay stores user and payee and credit card payment information for all Fleet sales conducted at Fleet auction houses. This information is needed to process payments, handle disputes, and process defaults for non-payment and non-removal.

MySales – MySales does not store any data in its application. It uses SASy sub-application sales and user data in the SASy database.

ReverseAuctions – ReverseAuctions stores all Buyer and Vendor information for procurement/reverse auctions conducted on the application.

3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

GSAAuctions uses past bidding history data based on product categories to identify target users to send marketing emails for upcoming sales. The bidders are selected by random (50% sampling) where marketing emails are sent on a daily basis. The results are used for marketing purposes only. This data is not used for normal business processes to determine bidder patterns, behavior, and aggregate or derive additional data about the user.

ReverseAuctions, ePay, SASy, MySales – Does not aggregate or derive new user data.

3.5 What protections exist to protect the consolidated data and prevent unauthorized access?

SASy FISMA system controls that protect data access, in transit, and at rest are documented in the SASY FISMA system SSP.

3.6 Will the system monitor the public, GSA employees or contractors?

SASy sub-application: Access to sensitive PII and Credit Card information by system users is logged and monitored and audited. This is used for FISMA and PCI DSS compliance.

GSAAuctions sub-application: Access to sensitive PII and Credit Card information is logged and monitored and audited. This is used for FISMA and PCI DSS compliance. IP Address information is stored during bidding, payment, and registration and is infrequently used by law enforcement in cases of actual or suspected fraud.

MySales, ePay and ReverseAuctions do not have a facility for users to view Credit Card data or sensitive PII.

- ePay sub-application: Locating or monitoring of individuals or users is not in use.
- MySales sub-application: Locating or monitoring of individuals or users is not in use.
- ReverseAuctions sub-application: Locating or monitoring of individuals or users is not in use.

3.7 What kinds of report(s) can be produced on individuals?

Access to sensitive PII and Credit Card information is logged and monitored and audited. This is used for FISMA and PCI DSS compliance. These logs are only available to system administrators.

3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

SASy Sub-Application Reports: SASy system produces Top 3 bidder report, register of remittance report, successful bidders report, defaulted bidders list.

- Top 3 bidders report: This report is produced for each sale/lot after the sale/lot is closed. The report lists the top 3 bidders for each sale/lot. The PII listed on this reports include bidder name, bidder company name (when available), address, email address, bidder #, and phone #.
- Register of remittance (ROR) report: This report is produced for every register (where payments are posted). ROR is an on-demand report which could be generated anytime after registers are closed. The PII listed in the report includes bidder name and last 4 of credit card # (for payments via credit card).
- Successful bidders report: This is an on-demand report which could be generated anytime after registers are closed. The PII listed in the report includes bidder #, bidder name and address.

- Defaulted bidders report: This report could be produced anytime. The report lists bidder # and bidder name.

All reports are accessible to the GSA Sales office as well as GSA-IT staff supporting SASy sub-application.

GSAAuctions Reports: The application does not produce any report with PII information.

MySales Reports: The application does not produce any report with PII information.

ePay Reports: The application produces one report which is receipt of the payments made. The receipt prints payment details including payee name.

ReverseAuctions Reports: The application does not produce any report with PII information.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

No data is collected beyond its stated purpose. Identity proofing / fraud prevention, payment processing, user notification, user defaults, etc.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?

Yes, The Personal Property Sales program SORN states “System records include: (1) Personal information provided by bidders and buyers, including, but not limited to, names, phone numbers, addresses, Social Security Numbers, birth dates and credit card numbers or other banking information, and (2) contract information on Federal personal property sales, including whether payment was received, the form of the payment, notices of default, and contract claim information.”

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

The GSAAuctions sub-application shares the bidder (Individual and Company) information for identity verification with Experian. The sharing of information is for the sole purpose of verifying the potential user’s identity so as to provide access to GSAAuctions platform. The information is shared via a secure HTTPS service.

The following PII information is shared by GSAAuctions sub-application to Experian.

- First and Last Name
- Company Name
- Home address
- Email address
- Telephone number
- Social Security Number or Tax Identification Number
- Credit card number (Optional)

The GSAAuctions, SASy and ePay sub-applications use Treasury’s Pay.gov interface to process payment for awarded auctions/sales. The information is shared via a secure HTTPS service.

The following PII information is shared with Pay.Gov.

- Name on Card
- City
- State
- Email address
- Credit card number

ReverseAuctions, ePay, MySales – Do not share any PII information to external users/organizations.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

Information is collected directly from individuals and companies . Below is how individual information is collected for each SASy system sub-application:

SASy Sub-Application: Individuals provide PII and PCI DSS information at the time of bidder account creation and payment for individuals that register, bid, and pay for surplus property sold on GSAAuctions or via other sale methods and elect to pay online in person, or over the phone and are stored in the SASy database. User data is manually entered via a SASy sub-application user or it is loaded into the system via a system interface.

MySales PII: Individuals provide PII information at the time of registration or account creation from person that post vehicles for online auctions and for Federal agency users that require visibility into the status of property being sold by GSA via an automated interface with the GSAXcess system and via system administrator user account creation.

ePay PII and PCI DSS: Individuals provide PII and PCI DSS information at the time of payment from the person that purchase vehicles at a GSA Fleet vehicle auction and are stored in the ePay database. Information is manually entered into the system by an ePay user.

GSAAuctions: Individuals and companies provide PII and PCI DSS information at the time of registration and payment from individuals that register, bid, and pay for surplus property sold on GSAAuctions and are stored in the GSAAuctions database. This information is manually entered by the user during registration, payment and profile updates.

ReverseAuctions: Individuals provide PII information at the time of registration from companies (potentially individuals) that register and bid on procurements on ReverseAuctions and are stored in the ReverseAuctions database.

4.4 Will the system, application or project interact with other systems, applications or projects, either within or outside of GSA? If so, who, how and is a formal agreement(s) in place?

GSAAuctions - Experian. The GSAAuctions sub-application shares bidder (Individual and Company) information for identity verification with Experian via the secure HTTPS PreciseID and BizID services. Data is transmitted electronically via a HTTPS service during user registration. The sharing of information is for the sole purpose of verifying the potential user's identity so as to provide access to GSAAuctions platform. A contract (Experian Data Use Addendum (DUA) to PO 4102859563 executed.pdf) is in place with Experian to provide PreciseID and BizID identity proofing services. The DUA document defines security and sharing parameters for information shared with and received by Experian. Experian will notify GSA of a suspected or confirmed security incident or breach of PII via email to the "HEAD SECURITY DESIGNATE" on file and other agency POCs as appropriate.

The GSAAuctions, and ePay sub-applications use Treasury's Pay.gov interface to process payment for awarded auctions/sales. Agreements "Pay.Gov GSA Auction ACT 082304 revised.doc" and Pay.Gov GSA Auction ACT 082304 revised.doc are in place with Treasury to provide electronic payment services. Treasury will notify GSA of a suspected or confirmed security incident or breach of PII via email to agency POCs on file and other agency POCs as appropriate.

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

Privacy Risk: Data leakage. Sensitive PII and PCI Data are sent to Experian and Pay.gov for the purposes of identity proofing and electronic payment. If the appropriate controls are not in place then data could be leaked externally.

Mitigation: Data is secured during transport via HTTPS TLS 1.2, RSA key exchange, and AES_256_GCM cipher. PII Data is secured at rest by: PANs are Key encrypted AES256 using the cryptographic libraries on the Crypto common appliance (based on the Microsoft Crypto SDK) and stored in SASy database. Disk encryption is used in addition to the column-level data key encryption using EMC SAN disk encryption. Pay.Gov Secures their cardholder data environment and complies with PCI DSS requirements. Experian maintains a high level of data security.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

The source of the data is the individual providing the data during registration, payment, or profile updates. Identity data is verified on GSAAuctions via Experian PreciseID and BizID services. If that fails, users can manually verify their identities with the Office of Personal Property Management. Email addresses, and email address changes are validated by an email activation link that is sent to the provided email address that the individual must click.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

GSAAuctions implemented identity proofing services to ensure that identity data provided by users was accurate and primarily not fraudulent. Experian services were chosen due to cost, ease of implementation, and Experian success providing similar services to other agency customers. These services mitigate risks associated with users attempting to register with another individuals information.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?

GSAAuctions/SASy/ePay/MySales/ReverseAucitons: GSA Office of Personal Property Management employees with system administration access, GSAAuctions Help Desk Contractors with Help Desk role, and GSAIT Development team members have access to PII data. New system users with privileged access must fill out a system specific User Access Request form which is reviewed and electronically signed by the account group owner defined in the GSAAuctions/SASy/ePay/MySales/ReverseAucitons Access Request Process and filed in the GSAAuctions/SASy/ePay/MySales/ReverseAucitons google shared team drive. The account is then created with the following parameters:

- Only the roles and permission necessary for that individual’s job function
- Restricted to least privileges necessary to perform job responsibilities
- Privileges assigned are based on the individual’s job classification and function

6.2 Has GSA completed a system security plan for the information system(s) or application?

The system security plan SASy has been completed for the ISSM review and approval. The current ATO has been extended until March 31, 2020

6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

The ClearPath environment that houses the SASy system has technical and physical security protections required for a FISMA Moderate system. The environment technical and physical and controls are detailed in the ClearPath SSP.

The SASy FISMA system has Technical controls that are documented in the SASy SSP:

- Identification and Authentication
- Access Controls
- Event auditing
- Encryption at rest and transport
- Vulnerability Scanning and Remediation

The SASy FISMA system has Managerial controls that are documented in the SASy SSP and on the SASy Google Team Drive:

- Security Training
- User access request procedures
- Annual user recertifications
- Key management procedures
- Audit Review, Analysis, and Reporting
- Security Assessments
- Incident Reporting and Incident Response Plan

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, what are they?

SASy Incident reporting plan and procedures are located in the SASY FISMA System Incident Response Plan.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

All SASY applications have role based access where users with need to know have access to the system. All GSA personnel undergo an annual Privacy training to ensure user privacy is maintained. Certain privileged users in SASy and GSAAuctions application have access to users SSN/TIN and credit card information. These privileged users' activities are logged as a security measure.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

Furnishing a social security number or tax identification number, as well as other data is voluntary, as is participation in the Personal Property Sales Program. Failure to provide this information, however, may result in ineligibility to purchase Federal personal property from the General Services Administration.

The GSAAuctions Terms and Conditions (T&C) provides a statement on the need to collect Social Security Number for Individuals and Tax Identification Number (TIN). Text provided from GSAAuctions T&C. The Debt Collection Improvement Act of 1996 is also referenced in the T&C as well as for fraud purposes. Credit Cards (CC) are not required to be provided during registration, however if bidder needs to pay using CC, they have to provide one. Other PII information is required for all applications in order to validate user identity as well as have accurate user information.

7.2 What procedures allow individuals to access their information?

GSAAuctions, ePay and ReverseAuctions provide a “Protecting Your Privacy” web page which has a Privacy & Security Notice section that references the Privacy Act of 1974 (5 U.S.C. Section 552a, as amended). SASy and MySales applications do not have privacy sections. A user can reach out to system POCs with a Privacy Act request or to system or program POCs if they want to access their information.

7.3 Can individuals amend information about themselves? If so, how?

Users can login to individual applications and update their information. They can also contact the respective application point of contacts to update their information.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

GSAAuctions and SASy need to maintain certain user account information with respect to sales contracts for legal purposes as well as data integrity for the set data retention period. If these conditions don't apply, users can contact respective application point of contacts to permanently delete their accounts.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application or project.

All GSA staff and contractors are required to take the mandatory annual Privacy training. GSA IT produces a report to identify individuals who have not taken the training and ensure the training is completed by everyone.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

There are no privacy risks with respect to Privacy awareness and training.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system, application or project ensure that the information is used in accordance with the stated practices in this PIA?

Control Safeguards: All SASy sub-applications are designed with role-based access. The business line determines and assigns application roles/permissions based on business need and need to know basis. During the User Access Request and Approval process, access forms are reviewed, signed and filled out to ensure that roles requested are the roles and permissions that are used for account creation.

Users provided access to the applications can access limited functionality based on user roles. External users do not have privileged access to any applications except ReverseAuctions. Remote access to the system and tape backups is not allowed.

Audit Safeguards: All SASy applications are hosted in the Clearpath environment where the ClearPath system records successful events, unsuccessful logon events, and failed usercodes and failed passwords attempts recorded as violations. All transactions create a database audit record. Host system file deletions and replacement logs are reviewed daily. All SASy sub-applications do not audit any user activity including user account manager activities. A few screens where SSNs and CCs are viewable are audited in SASy and GSAAuctions sub-applications. User actions on these screens are saved as history / audit records. These audit records are created on every visit to the page(s). In the event of a suspected PII incident or upon request a system administrator can review and report on all user accesses to these records via the access audit records. All user web transactions (create, update and delete) generate a database audit record. In the event of a suspected PII incident or upon request a system administrator can review and report on the database audit records.

SASy sub-application: Role-based access proves access to business function for specific user roles. For example, the System Administrator has access to create, change, lock and unlock users. The roles are approved and assigned by account managers (business line and GSA IT). GSA users have privileges to certain screens based on their assigned roles. The functions of user management are not audited. Social Security Number (SSN) and Credit Card (CC) Numbers are encrypted using crypto mechanism. SSNs and CCs are visible in its entirety in certain screens for certain roles on a need-to-know basis. The screens with SSNs and CCs visible in its entirety are audited. Invalid user login attempts are logged on the user account as violations. Credit Card and SSN/TIN access/views are logged in audit records.

ePay sub-application: Role-based access proves access to business function for specific user roles. For example System Administrator has access to create new users, change user levels, deactivate and activate users. The system administrator has access to non-privileged functions. ePay application account management activities are not audited. Users are established based upon their role and actions that they will need to access within the system. The least privilege to accomplish those necessary tasks is given (AH User, AH Admin, Sys Admin role setting).The application does not audit the execution of privileged functions. ePay records unsuccessful login attempts and locks the account after 3 unsuccessful attempts. No other events are audited by the application.

GSAAuctions sub-application: Role-based access proves access to business function for specific user roles. For example System Administrator has access to create, change, default, un-default, Expire, Compromise, lock and unlock users. The application shows bid history at the sale/lot level, it does not show bidding history beyond a sale/lot level. The roles are approved and assigned by account managers (Business line and GSA IT).

Limited automatic audit functionality exists, specifically, Admin actions on user accounts during

1. Change of status of locking, unlocking, expiring, compromising, defaulting and undefaulting actions is captured.
2. Role changes on accounts.

GSA users have privileges to certain screens based on their assigned roles. History records log limited system administrator functions such as locking and unlocking accounts. Social Security Number (SSN) and Credit Card (CC) Numbers are encrypted using key encryption. SSNs are visible in their entirety on certain screens for certain roles on a need-to-know basis. The screens with SSNs visible in their entirety are audited. Invalid user login attempts are logged on the user account as violations. User activity is audited for limited user actions including user account manager activities. Access to the screens where SSNs are viewed are saved as history/audit records. These audit records are created on every visit to the page(s).

MySales sub-application: MySales application allows roles to be assigned to user accounts. Roles are assigned by user account managers and are associated with business functions. If a non-privileged role is not assigned to a privileged account, the user will not be able to access the business function. MySales does not audit the execution of privileged functions. MySales records unsuccessful login attempts and locks the account after 3 unsuccessful attempts. No other events are audited by the application.

ReverseAuctions sub-application: Privileged accounts created in Reverse Auctions - The application records and creates history records for account creation, modification, enabling, disabling and removal actions.

eBuy vendor and Buyer accounts - Buyer and Schedule Vendor accounts are maintained by GSA Vendor Support System. Role based access provides access to business functions for specific user roles. The system administrator role has access to non-privileged functions. GSA users have privileges to certain screens based on their assigned roles. The auditing of system administrator functions is not implemented. Company Tax identification Number (TIN) are encrypted using crypto mechanism. The TIN numbers are required by vendors to register as Open Market vendors to participate in Open Market auctions. TIN numbers are not visible on any of the application screens. Other user activities including user account manager activities, valid user login attempts, data deletions, and data changes are logged.

Agreement Safeguards: Interconnection Security Agreements (ISAs), MOUs and other information sharing agreements are drafted by GSA if they are the information or service provider. All GSA information sharing agreements contain data sensitivity sections that discuss the confidentiality of the information being exchanged, if the information contains PII, and how the information is protected. If GSA is the recipient or consumer of the ISA, MOU or other information sharing agreement it is incumbent upon the SASy project team to make sure that the data sensitivity of the information being shared is properly documented in the agreement. The SASy Project Manager drafts or reviews the information sharing agreements and then sends the agreement to the SASy ISSO for review. If it is unclear if the agreement contains PII then the SASy Project Team consults GSA’s Privacy Office to make a determination on the sensitivity of the data being shared and if the protections in place are sufficient to safeguard it. When the draft information sharing agreement is complete, the agreement is sent to the SASy ISSM for review. When the agreement is finalized by both parties, it is first signed by the service / information consumer System Owner and Authorizing Official and then by the service / information provider System Owner and Authorizing Official. The signed agreement is distributed to both parties and archived in the Team Drive in the Security Interconnection

Security Agreement (ISA/MOU) folder. The interconnection is documented on the System Interconnections tab of the SASy FISMA System SSP google sheet. Agreements are reviewed annually and can be terminated upon 30 days advance notice.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

As stated in 9.1 all precautions are taken to safeguard PII information and audited certain actions with respect to privacy data use. Privileged users are only granted roles and permission necessary for that individual's job function, restricted to least privileges necessary to perform job responsibilities, and the privileges assigned are based on the individual's job classification and function.

[1] OMB Memorandum *Preparing for and Responding to a Breach of Personally Identifiable Information* (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.