Privacy Impact Assessment

Sales Automation System

June 11, 2018

Privacy Impact Assessment (PIA) for the

GSA IT Acquisition IT Services

Asset and Transportation Management Division

Sales Automation System (SASy)

June 8, 2018

Contact Point: Katie Jaworski ISSM
GSA-IT
Services ISSO Support Branch (IST)
202-501-1302

Abstract

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,
- MySales,
- ePay, 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 ITS National Information Technology Commodity Program (NITCP) in the procurement of GSA Schedule and BPA commodities and services.
- Veterans Affairs (VA) in the procurement of VA schedule commodities and services.
- Department of Homeland Security (DHS) in the procurement of DHS First Source BPAs.
- All agency buyers of BPA, MAS and Open market commodities and services.

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 10 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, Reports.fss.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 is secured at rest by: 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 Ancillary Financial Applications (GSA AFA) via a secure file transfer. The Sales Automation System (SASy) sends register of remittance files to GSA Finance on a nightly basis. The register of remittance files includes bidder first name, last name, and encrypted credit card numbers.

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 address 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) and 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: BSP Logical Data Environment (BSP LDE), eBuy, Enterprise Service Oriented Architecture (eSOA), FedBizOpps (FBO), GSA Advantage, JUpload, 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 ReverseAucitons 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 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the application in question?

The Federal Property And Administrative Services Act of 1949. The act was designed, in part, to increase the efficiency and economy of Federal government operations with regard to the procurement, utilization and disposal of property.

The Federal Property And Administrative Services Act of 1949 Section 484 - "Disposal of Surplus property" Provides that the care and handling of surplus property pending its disposition, and the disposal of surplus property, may be performed by GSA or any executive agency designated by the Administrator.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) applies to the information?

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

1.3 Has a System Security Plan (SSP) been completed for the information system(s) supporting the application?

The last ATO was issued on July 23, 2015 for Sales Automation System (SASY). The SSP is currently being updated for upcoming security assessment.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

A SASy FISMA system retention schedule does not exist in NARA. The record retention schedule is based off 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

See section 5.1 for more details on SASy records.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Not Applicable

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the application collects, uses, disseminates, or maintains.

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 – Captured following information during payment process

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

MySales – Collects following information

- 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

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 verify 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 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 email for upcoming sales. The bidders are selected by random (50% sampling) where marketing emails are sent on a daily basis. Any bidding history to date has not 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 – Open Market vendors self-register in the application. Sam.gov is used to verify if a vendor is in active status.

2.2 What are the sources of the information and how is the information collected for the application**?**

GSAAuctions – Individual and Company bidders self-register in GSAAuctions. Administrator user accounts are created by system owners/ administrators.

ReverseAuctions – Open Market vendors self-register in the application. Sam.gov is used to verify vendor's are in active status. Administrator user accounts are created by system owners/ administrators.

SASy – Regional sales office creates bidder records for bidders participating on offline sales. Administrator user accounts are created by system owners/ administrators.

ePay - Administrator user accounts are created by system owners/ administrators. Auction house users are created by administrators.

MySales - Administrator user accounts are created by system owners/ administrators. Fleet sales accounts are created by administrators. Agency accounts are created by batch process which is initiated by GSAXcess.

2.3 Does the application use information from commercial sources or publicly available data? If so, explain why and how this information is used.

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 Experian service BizId, GSAAuctions sends company TIN, company name and address to get a decision. The results are saved in GSAAuctions.

ReverseAuctions – Does not use any information from commercial sources

ePay - Does not use any information from commercial sources

MySales - Does not use any information from commercial sources

SASy - Does not use any information from commercial sources

2.4 Discuss how accuracy of the data is ensured.

Commercial Products: Experian provides decision based primarily on 100% SSN match with individual name for individuals and 100% TIN match with company name for companies.

SASy, GSAAuctions, ePay, MySales and ReverseAuctions sub-applications:
The databases define datasets or tables with unique indexes based on business need. For example the users table defines an index for users by username defining each record in users table to relate to one specific user. All applications lookup requested information on key fields like username. For example when users login with a user name and password, the user name is searched in the users's table looking for an exact matching record with user name. Once the user record is identified, the password is matched to identify 100% user match.
The Quality Assurance (QA) step during the software development process performs several data validity tests (unit, regression and integration) to verify data filled in the forms is saved in the databases correctly.

Section 3.0 Uses of the Information

The following questions require a clear description of the application's use of information.

3.1 Describe how and why the application uses the information.

GSAAuctions: 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 are saved in GSAAuctions. GSAAuctions also holds credit card payment information for all payments made for awarded auctions.

SAsy – SASy holds Sales and bidder information for all sales conducted by Office of Personal Property and Fleet.

ePay – ePay holds credit card payment information for all Fleet sales conducted at Fleet auctionhouses

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

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

3.2 Does the application use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how GSA plans to use such results.

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 any bidder pattern or behavior. Using this data for other business process requires application changes which need to authorized by the business line and GSA-IT. To our knowledge there is no approved process to identify predictive pattern. The bid history data has never been purged and it is available to all approved SASy user (with documented access request forms).

ReverseAuctions, ePay, SASy, MySales – Does not use any data for predictive analysis.

3.3 Are there other components with assigned roles and responsibilities within the system?

Experian service PreciseId and GSAAuctions sends SSN, name, address and optionally credit card numbers of individuals to get a decision. For Experian service BizId, GSAAuctions sends Company TIN, company name and address to get a decision. The results are saved in GSAAuctions.

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.

GSAAuctions & ePay – uses treasury's Pay.Gov OCI service to process credit-card payments. The GSAAuctions & ePay 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.

3.4 Privacy Impact Analysis: Related to the Uses of Information

The business line and the branch manager define roles and responsibilities associated with each permission given to the users. All sub-applications (GSAAuctions, SASy, ReverseAuctions, ePay and MySales) use access request forms to initiate and define access requirements for each user. User accounts are created based on the roles defined on the access request forms. Based on that, access is only granted to required users. Annual Privacy Training provides guidelines for the use of sensitive information. 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 the SASy database. Disk encryption is used in addition to the column-level data key encryption using EMC SAN disk encryption.

The transaction reports are produced and are available for management review on a daily basis. The transaction reports are reviewed daily by the branch chief and system owner on a daily basis. The report provides report on file removals and file replaces. Sometimes some source files or web content could be accidentally removed or replaced. The logs provide this information. These issues are identified from the report and are corrected as soon as possible and users are informed.

It is the business line and the branch manager's discretion to remove the permission assigned or the user id. Each user id and roles/permission is reviewed annually and certified by the managers.

Privacy Risk: SASy users are authorized by the business line and the branch manager with necessary permissions to receive data, files and upload the database server and certify annually, there is no risk associated with the function. However, if the SASy database or account credential/information is compromised, then there is a potential risk involved. Compromised Account risk includes exposure to information relating to other user. On the GSAAuctions side, the bidding history is exposed to a Sale/lot level. Bidding history is not exposed beyond a Sale/lot.

Mitigation: User certification is done annually after careful review of each and every LID and their associated permission**.** The SASy database is secured with a monthly scan of the server and any findings are fixed within the timeframe. 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.

Section 4.0 Notice

The following questions seek information about the application's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the application provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

GSAAuctions users are notified during the registration process by the GSAAuctions Terms & Conditions of what data will be collected and retained as part of the registration process. 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 account are created upon request to conduct certain job duties.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the application?

The GSAAuctions self-registration process for bidders provides users a choice to accept or reject the GSAAuctions terms and conditions. Users declining to accept the terms and conditions are declined from continuing the registration process. Users accepting the terms and condition can continue to register and provide personal information.

GSAAuctions also sends marketing email to bidders based on past bidding history. The bidders are provided an opt-out option in the marketing email for opting out of the marketing campaign. By default registered users are opted-in. The marketing email provides an option to opt-out.

ReverseAuctions – General Terms and Conditions are posted on the website regarding open market vendor registration need to participate in Solicitation process.

SASy, ePay & MySales – User account are created on request to conduct certain job duties. User can request their account to be locked or disabled.

Section 5.0 Data Retention by the application

The following questions are intended to outline how long the application retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The retention period applies to all sub-applications.

The Office of Personal Property has 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 the 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 has not 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:

"3. 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."

5.2 Privacy Impact Analysis: Related to Retention

The information in this section applies to all sub-applications.

Privacy Risk: The information is stored in secured enterprise storage environment and the SASy database is protected with access controls. Data at rest and backups on tape are encrypted using EMC SAN disk encryption. In addition, certain PII data (TIN and credit card numbers) are key encrypted using Crypto common appliance (based on the Microsoft Crypto SDK). Therefore no significant privacy risk expected. The bidding history data is not purged to date.

Mitigation: 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 the SASy database. Disk and tape backup encryption is used in addition to the column-level data key encryption using EMC SAN disk encryption.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the application information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 Is information shared outside of GSA as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The GSAAuctions sub-applicaton 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 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 following PII information is shared by to Pay.Gov.

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

ReverseAuctions, ePay, MySales – Does not share any PII information to external users.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The Personal Propery 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."

6.3 Does the application place limitations on re-dissemination?

Information shared by GSAAuctions with Experian has a limit of one attempt for individuals (SSN and Name check) and multiple attempts for Company (TIN and Company name check). Companies are provided multiple attempts for same TIN with different accounts. Credit Cards payment can be attempted/submitted only once for a particular contract.

6.4 Describe how the application maintains a record of any disclosures outside of the Agency.

The data sent to Experian for user authentication is available to designated GSA users via web portal. The processed data history and information is available for review via the web portal.

The credit card processing data sent to pay.gov is available to designated GSA users via the web portal. The card processing data information is available for review via web portal.

6.5 Privacy Impact Analysis: Related to Information Sharing

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.

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.

Privacy Risk: The contract with Experian and ACT agreement with Pay.Gov covers the risks.

Mitigation:

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

GSAAuctions

- Registered bidders can access their personal, credit card, contact, password information through the "My Preferences" tab.
- Eligibility of Bidders: Bidders must be at least 18 years of age. Bidders will be required to provide their birth date at registration. A bidder's birth date will be used only to verify bidder's eligibility. This information is protected by the Privacy Act, 5 U.S.C 552a.

SASy

- Authorized users are able to review their information on the "Dashboard" screen in SASy.

MySales

- Authorized users are able to review their information by selecting "Update Your User Information."

ePay

- Non-privileged users are not able to change their information. Only system administrators have access to update user information via Create/Change user screen.

ReverseAuctions

- System Administrator accounts are created in the application. Open Market Vendors self-registerin the application. These 2 user groups can change their user information via the MyPreferences function.
- All other Buyers and Vendors users accounts are managed in GSA eBuy. Their user information is managed in GSA eBuy and cannot be altered in ReverseAuctions.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

GSAAuctions

- Unsuccessful attempt at registration for Individual:
  - If user makes a mistake while entering TIN during registration and the system fails their registration, user will be required to re-register since the system does not correct TIN information. If information other than TIN or full name was mis-typed, the user will be able to correct it in their profile. The user must contact the system owner for assistance in making any corrections to the name (see below for that process and requirements.
- Unsuccessful attempt at registration for Company:

- If user mis-types the TIN during registration and the system fails their registration, user will be required to re-register since the system does not correct the TIN information. If information other than TIN or full name was mis-typed, the user will be able to correct it in their profile. The user must contact the system owner for assistance in making any corrections to the name.

- Successful Individual registrants:
  - Users can correct/change their address and email address within the "My Preferences" section.
  - Users can request a change to their full name with proof of ID (ie. Marriage certificate or driver's license with name change reflected).
- Successful Company registrants:
  - Users can correct/change their address and email address within the "My Preferences" section.
  - Users can request a change to their full name with proof of ID (ie. Marriage certificate or driver's license with name change reflected.) If a company name change is requested, proof of name change must be presented. If the new company name does NOT match the TIN that was originally registered, the user will have to re-register the new company.

SASy

- Each zonal office is assigned a Central Office employee to assist with administrative assistance in SASy. If any corrections need to be made, the supervisor can email the Central Office employee to request a change to the user's profile.

MySales

- As a main function in the system, the "Update Your User Information" function is easily accessible to users for easy updating.

ReverseAuctions

- MyPreferences functions allows users to update user information.

7.3 How does the application notify individuals about the procedures for correcting their information?

GSAAuctions

- Unsuccessful Individual and Company Registrants are notified about failed registration via email immediately following the registration attempt. They are also provided with details on the requirements for successful registration.
- The FAQ section provides customers with guidance on how to correct information.
- The Tutorial tab is available for all customers to review and explains how to change/update information.
- The GSAAuctions.gov Terms and Conditions explain to customers that they are responsible for ensuring email addresses and registration information are kept up-to-date.
- Successful registrants have the "My Preferences" tab easily accessible to them while logged into the GSAAuctions.gov application.

SASy

- Although the application itself does not notify users, users are aware of who their Central Office point of contact is if ANY information needs to be updated. All SASy users are GSA users. They follow the chain of command or their central office contact.

MySales

- There is a tutorial that can show the area where a customer could update their information.

ePay

- The application does not notify users but the users are informed by the System Administrators to contact them to correct user information.

ReverseAuctions

- Vendor Tutorials are available to help Vendors navigate the application as well as update their personal information.

7.4 Privacy Impact Analysis: Related to Redress

The application does not provide any redress methods other than information provided in Section 7.3. However, users can contact the central office business line concerning data maintained by the applications and means to correct it.

Privacy Risk: None, because self-registrant users can update their information on the GSAAuctions and ReverseAuctions. In other sub-applications users can contact the system administrators or supervisors to update their information.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

All applications are hosted on the Clearpath environment where system records successful events, unsuccessful logon events, failed usercodes and failed passwords recorded as violation. 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. Users actions in these screens are saved as history / audit records. These audit records are created on every visit to the page(s). All web transactions (create, update and delete) generate a database audit record.

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-priviledged 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 priviledged 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 function like locking, unlocking accounts. Social Security Number (SSN) and Credit Card (CC) Numbers are encrypted using crypto mechanism. SSNs are visible in its entirety in certain screens for certain roles on a need-to-know basis. The screens with SSNs visible in its entirety are audited. Invalid user login attempts are logged on the user account as violations. User activity is audited for limited user action including user account manager activities. The screens where SSNs are viewable 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, 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 bases access proves access to business function 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 applictaion screens. Other user activities including user account manager activities, valid user login attempts, data deletions, and data changes are logged.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the application.

GSA offers annual privacy and security training. All users with access to PII are GSA employees or GSA Contractors who have taken the Privacy and Security Training.

8.3 What procedures are in place to determine which users may access the information and how does the application determines who has access?

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 Approval process, access forms are filled in to determine roles and permissions which are used for account creation.

Users provided access to the applications can access limited functionality based on user roles. See section 8.2 for audited events. External users do not have priviledge access to any application except ReverseAuctions. Buyers in ReverseAuctions application can be from other federal agencies who have access to creating procurement auctions and awarding for their auctions. Remote access to the system and tape backups is not allowed.

8.4 How does the application review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within GSA and outside?

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.