



Beta.SAM.gov

Privacy Impact Assessment (PIA)

May 3, 2021

POINT of CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

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

Stakeholders

Name of Information System Security Manager (ISSM):


- Joseph Hoyt
- joseph.hoyt@gsa.gov

Name of Program Manager/System Owner:

- Arunkumar Reddy
- arunkumar.reddy@gsa.gov


Signature Page

Signed:

DocuSigned by:

CA8EF810EDA7425...
Information System Security Manager (ISSM)

DocuSigned by:

D2FE0F442BBD486...
Program Manager/System Owner

DocuSigned by:

171D5411183F40A...
Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/10/2020	Privacy Impact Assessment Update	2.0
04/20/2021	Update for the New Template	3.0

Table of contents

SECTION 1.0 PURPOSE OF COLLECTION

- 1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
- 1.2 Is the information searchable by a personal identifier, for example a name or Social Security number? If so, what Privacy Act System of Records Notice(s) applies to the information being collected?
- 1.3 Has an 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.
- 1.4 What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.

SECTION 2.0 OPENNESS AND TRANSPARENCY

- 2.1 Will individuals be given notice before to the collection, maintenance, use or dissemination and/or sharing of personal information about them? If not, please explain.

SECTION 3.0 DATA MINIMIZATION

- 3.1 Why is the collection and use of the PII necessary to the project or system?
- 3.2 Will the system create or aggregate new data about the individual? If so, how will this data be maintained and used?
- 3.3 What controls exist to protect the consolidated data and prevent unauthorized access?
- 3.4 Will the system monitor members of the public, GSA employees, or contractors?
- 3.5 What kinds of report(s) can be produced on individuals?
- 3.6 Will the data included in any report(s) be de-identified? If so, how will GSA aggregate or de-identify the data?

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

- 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, maintenance, use, or dissemination?
- 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 GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

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 (SSP) for the information system(s) supporting the project?

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

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

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, 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?

SECTION 8.0 AWARENESS AND TRAINING

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

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about the System for Award Management (Beta SAM). The Integrated Award Environment (IAE) may, during its mission and business functions, collect personally identifiable information (“PII”) about individual who do business or consume IAE products and services. PII refer to any information¹ 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, maintains, disseminates uses, secures, and destroys information in ways that protect privacy. This PIA comprises 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 codified in the Privacy Act of 1974.^[2]

A. System, Application, or Project Name:

Beta System for Award Management (Beta SAM)

B. System, application, or project includes information about:

Beta SAM is the trusted, essential place to seamlessly connect to the business of government. As such, Beta SAM collects information on entities registering to do business with the U.S. government in accordance with Federal Acquisition Regulation (FAR) Subpart 4.11 and Title 2 of the Code of Federal Regulations (2 CFR) Subtitle A, Chapter I, and Part 25. Part of the registration data collected from entities which pay U.S. taxes is the Taxpayer Identification Number (TIN). The TIN is usually the entity’s Employer Identification Number (EIN). However, sole proprietors and single-member limited liability companies can elect to use their Social Security Number (SSN) as their TIN. The system also collects as part of registration process, names of (First, Last and Middle) individuals registering as Sole Proprietorship and addresses of entities and individuals registering to do business with the U.S Government.

C. For the categories listed above, how many records are there for each?

About 1.4 million record estimated for all the categories listed above

¹OMB 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.”

D. System, application, or project includes these data elements:

Beta SAM provides detailed, public descriptions of federal assistance listings available to State and local governments (including the District of Columbia); federally recognized Indian tribal governments, Territories (and possessions) of the United States; domestic public, quasi- public, and private profit and nonprofit organizations and institutions; specialized groups, and individuals. There are different types of award data, or “domains”. A user will be able to search across all domains or choose a specific domain to search within a specific data set. The table below provides a view of detailed records for all domains:

Domain	Description
Assistance Listings	Find assistance listings by entering a keyword, Catalog of Federal Domestic Assistance (CFDA) number, or agency name into the search field.
Contract Opportunities	Find contract opportunities by entering a keyword, solicitation ID, or an agency name into the search field.
Contract Awards	Find contract award data by entering a keyword, award type, North American Industry Classification System (NAICS) Code, Product Service Code (PSC), or DUNS (“data universal numbering system”).
Entity Registrations	Find entity registrations by entering an entity’s name into the search field. The search filter will automatically display “active” entities, but you can also switch to view only inactive results.
Entity Exclusions	Find exclusions associated with a particular entity by entering the entity’s name, DUNS number, or Commercial and Government

	<p>Entity (CAGE) code. To search for a person, type in his or her name. Be sure to confirm that you've found the correct person—it's easy to misidentify someone if he or she has a common name. If no exclusion record is found for the entity, the entity does not have an active exclusion in SAM.</p>
Federal Hierarchy	<p>Enter a department or sub-tier.</p> <p>Use the Federal Hierarchy filter to narrow your results.</p>
Wage Determinations	<p>Find applicable Service Contract Act (SCA) and Davis-Bacon Act (DBA) wage determinations required for each contract action by entering a wage determination (WD) number or using the filters to narrow down your results by geographic location.</p>
Contract Data Report	<p>Find and run <i>standard</i>, <i>static</i>, <i>administrative</i>, and <i>ad hoc</i> contract data reports. Users may use the reports to search public award data to find competitive information and build their business pipelines. Users can learn when existing contracts expire and to help identify potential subcontracting opportunities. Federal agencies use this data to measure, analyze, and report on how federal contracting affects the U.S. economy and the success of policy.</p>

Overview

Beta SAM is a modernization solution of the Integrated Acquisition Environment (IAE); a Presidential E-Gov initiative and key component of the modernized GSA Technology Platform created to simplify, unify, and streamline the complex acquisition process for Federal Awards. The modernization solution embraces the 21st century architectures, agile development, and

user-centric design approaches to create a transparent, secure, efficient, and accessible environment. It's designed to offer a comprehensive suite of capabilities in support of the strategic goals of the GSA IAE and provides federal, public, and industry users; improve efficiency of the acquisition services and data through a single, web-based platform, requiring single sign-on, and containing separation of duties for multiple agencies and vendors with many agency requirements.

The modernization initiative serves to streamline and manage the acquisition functions common to all agencies through the reuse, data sharing, linking systems and making data accessible to all. Beta SAM is composed of many functionalities or capabilities that facilitate the Federal award and acquisition process which are previously provided by disparate legacy systems are codified into domain providing the following functionalities.

1. **Contract Opportunities** - Provides information on business opportunities for the federal government.
2. **Wage Determination** - Single location for federal contracting officers to use in obtaining appropriate Service Contract Act (SCA) and Davis-Bacon Act (DBA) wage determinations (WDs) for each official contract action
3. **Assistance Listings** - Government-wide compendium of Federal programs, projects, services, and activities that provide assistance or benefits to the American public. It contains financial and nonfinancial assistance programs administered by departments and establishments of the Federal government.
4. **Contract Data (Databank)** - Modernized reporting functionality of beta SAM specifically designed to streamline data flow and the reporting capability using MicroStrategy, an FCS service. The Databank serves as the authoritative source for report data. Databank utilized kinesis to aggregate, seamlessly process, ingest, and analyze real-time data from various sources to provide timely insights and react quickly to user request.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

For the Entity Management functional area of Beta.SAM, the authorities for collecting the information and maintaining the system are the Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c).

For the exclusions portion of the Performance Information functional area, the authorities for collecting the information and maintaining the system are FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989).

1.2 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?

Data is retrieved by searching against information in the record, including, but not limited to, the person's or entity's name, DUNS Number/Unique Entity Identifier (UEI) Number, SSN and TIN. GSA/GOVT-9 System for Award Management SORN apply to the information being Collected. Searching for registration records by TIN is limited to Federal Government users. Searching for exclusion records by SSN or TIN requires an exact name match.

1.3 Has an 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.

Information Collection Request (ICR) has not been submitted for the information system (Beta SAM).

1.4 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.

System records are retained and disposed in accordance with GSA records maintenance and disposition schedules, the requirements of the Recovery Board, and the National Archives and Records Administration. For the Entity Management functional area, Beta.SAM allows users to update and delete their own entity registration records. For the exclusions portion of the Performance Information functional area, electronic records of past exclusions are maintained permanently in the archive list for historical reference. Federal agencies reporting exclusion information in Beta.SAM follows the agency's guidance and policies for disposition of paper records.

SECTION 2.0 OPENNESS AND TRANSPARENCY

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

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

For the Entity Management functional area, individuals are aware that Beta.SAM contains a record on them because they created the record through a self-registration portal. For the

exclusions portion of the Performance Management functional area, individuals receive prior notification of their exclusion from Federal procurement and non-procurement programs.

SECTION 3.0 DATA MINIMIZATION

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

Beta SAM collects necessary information from individuals and entities seeking to do business with the U.S Government. The information is required to create a profile/record for the entity/individuals, establish and validate the applicant's identity, determining the eligibility of various awards/grants/programs/benefits and in furtherance of the Beta SAM mission and business processes.

The exclusion records on individuals contain information that is not publicly displayed (e.g., street address information, as well as the SSN or TIN). Agencies disclose the SSN of an individual to verify the identity of an individual, only if permitted under the Privacy Act of 1974 and, if appropriate, the Computer Matching and Privacy Protection Act of 1988, as codified in 5 U.S.C. 552(a).

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

No new data will be created or derived based on the information collected.

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

In accordance with the Federal Information Security Modernization Act of 2016 (FISMA), all GSA system must receive a signed Authority to Operate (ATO) from a designated GSA official. The ATO process includes a rigorous assessment of security controls, a plan of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program to maintain the security posture of the information system.

FISMA controls implemented contains a combination of management, operational, and technical controls, and include the following control families: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment,

system and services acquisition, system and communications protection, system and information integrity, and program management.

The following specific controls are implemented to protect the confidentiality, integrity and availability of the Beta Sam system and the data transmitted, processed, and stored within the environment of operation:

Management Controls

- Certification, Accreditation and Security Assessments (CA)
- Planning (PL)
- Risk Assessment (RA)
- System and Services Acquisition (SA)

Operational Controls

- Awareness and Training (AT)
- Configuration Management (CM)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA) Media Protection (MP)
- Physical and Environment Protection (PE)
- Personnel Security (PS)
- System and Information Integrity (SI)

Technical Controls

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)
- System and Communications Protection (SC)

Privacy Controls

- Authority and Purpose (AP)
- Accountability, Audit, and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)

Additionally, all GSA employees are required to take annual security awareness training, which addresses privacy and handling of PII data. GSA also maintains rules of behavior for employees who use GSA systems and limits access to PII by employing role-based access (only allowing access to users who need PII to perform their duties).

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

No, Beta SAM system is not designed to monitor the public, GSA employees or contractor. However, Beta.SAM resides in a Container-as-a-Service (CaaS) Cloud environment. There are various monitoring tools configured to monitor, and log/audit the system applications to enhance the incident management capabilities.

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

Beta SAM does not produce any reports on individuals. All reports are pertaining to contracts (contract data reports), grants, or FAR requirements. In the event of a sole proprietor, the report will be pertaining to contracts, grants, or FAR requirements but may contain PII, if PII is used in the sole proprietor's business operations.

3.6 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?

No, data included in reports will not be de-identified.

SECTION 4.0 LIMITS ON USING AND SHARING 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?

Beta.SAM is used today to research, manage, administer, and report on federal awards in one environment hosted on a secure AWS Cloud Platform (CaaS) to provide a consistent, dependable access to reliable, accurate and timely data and business intelligence in a transparent manner.

Data is retrieved by retrievable by searching against information in the record, including, but not limited to, the person's or entity's name, Unique Entity Identifier (UEI) number, SSN and TIN. GSA/GOVT-9 System for Award Management SORN apply to the information being Collected. Searching for registration records by TIN is limited to Federal Government users. Searching for exclusion records by SSN or TIN requires an exact name match.

Beta SAM maintains the Government wide system of records to enable Federal agencies to determine who is registered to do business with the Federal Government, and to identify individuals who have been excluded from participating in Federal procurement and non-procurement (financial or non-financial assistance and benefits programs), throughout the

Federal Government. In some instances, a record may demonstrate exclusion that applies only to the agency taking the action, and therefore does not have Government wide effect. The purpose of the exclusions is to protect the Government from non-responsible contractors and individuals, ensure proper management throughout the Federal government, and protect the integrity of Federal activities.

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?

Yes. Federal agency Contract Writing Systems (CWS), grants management systems, and financial systems will all use data from Beta.SAM. They go through a data access request process to allow them certain levels of data. The data is provided over encrypted connections and are either SFTP or web services (XML) and managed through role management. Part of the access process includes a Non-Disclosure Agreement and System Authorization Access Request (System Account) which is agreed to by the requestor during the data access request process and includes user responsibility regarding the data.

Also, users (Federal and Non-Federal) may access beta SAM data using a system account. Federal and Non-Federal users must submit a System Account Application to request access to Beta SAM. The application is reviewed for business justification, need to know, valid authorization and other security requirements. Once approved users are granted access to Beta.SAM.gov APIs. The application process is through an automated self-service portal on Beta.Sam.gov to request a system account.

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)?

Entity records are created by the person or entity wishing to do business with the government. Exclusion records are created by Federal agency suspension and debarment personnel.

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

Beta.SAM may interact with other systems either internally or externally to GSA there must be an MOU/ISA established for such interaction. The MOU/ISA is reviewed and approved by both partnering agencies. On the GSA side, the Beta.SAM MOU/ISA is approved by the ISSO and the Authorizing Official (AO) for Beta.SAM. Data is transmitted either via a persistent pipe (TI, T3, VPN, SFTP, etc.) or a non-persistent pipe (internet, web portal, http, etc.)

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, maintained, used, or disseminated be verified for accuracy and completeness?

To verify accuracy, system validation rules exist. Entity-entered TINs are validated by the IRS to ensure the TIN and Taxpayer Name provided matches the TIN and name control on file with the IRS. Access to edit an entity record is controlled through roles and permissions.

For completeness, system validation rules ensuring required fields are populated correctly are in place. A record cannot be completed without all mandatory fields being completed.

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?

Beta.SAM has a System Security Plan (SSP) as well as a user guide that thoroughly documents access control, roles, and permissions. Access to data in the system, application, or project is restricted to authorized user only commensurate to their approved role and permission.

Roles are based on the required function of the users, and include the entities, government procurement personnel, government debarment personnel etc.

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

Yes, a formal documented System security Plan (SSP) is completed for the information system and constantly being updated to reflect its current state in maintaining the security posture. Beta SAM Information system is categorized as “MODERATE” using the Federal Information Processing Standard Publication (FIPS199), Standards for Security Categorization of Federal Information and Information Systems in relation to the confidentiality, integrity and availability of the system and data processed, transmitted, or stored. Based on this categorization, GSA implements security controls from NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations” from the moderate security baseline, tailor, supplement/enhance those controls to secure its systems and data.

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

Beta SAM resides in the GSA FAS Cloud Services (FCS) Platform as a Service (PaaS)/Container as a Service (CaaS) Mode 3 model, ultimately leveraging the Amazon Web Services (AWS) East/West Region. Also, the information system has implemented technical, operational, management and privacy control to secure the system and its data and maintain the security posture of the system.

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

Beta.SAM resides in the AWS Cloud environment (Container as a Service) with various automated mechanism in place for logging/auditing using Cloud Watch, Slunk, and application monitoring (New Relic) for incident management in accordance with the GSA policies and procedures for handling security incidents. Responsible system and technical officers report any potential incidents directly to the relevant Information Systems Security Officer. This Officer coordinates the escalation, reporting and response procedures on behalf of GSA.

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 do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

Individuals do not have opportunities to opt out or decline to provide information to Beta.SAM. Most of the data collected by the system is related to agency entities which are provided by a company pursuant to applicable laws and regulations rather than directly from users. Additionally, data collected by Beta.SAM entities is related to their access and use of the system and is collected through use of the system.

7.2 What procedures allow individuals to access their information?

Since individuals/entities created the entity registration record in Beta.SAM through a self-registration portal, there are no restriction or limitation to managing such data. Users can delete, update, or amend the record at will. However, individuals can contact the system manager with questions about the operation of the Entity Management functional area. Requests from individuals to determine the specifics of an exclusion record included in Beta.SAM should be addressed to the Federal agency POC identified in the exclusion record.

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

Yes, since individuals create the entity registration record in Beta.SAM through a self-registration portal, there are no restriction or limitation to managing such data. Users can delete, update, or amend the record at will. However, individuals can contact the system manager with questions about the operation of the Entity Management functional area. Requests from individuals to determine the specifics of an exclusion record included in Beta.SAM should be addressed to the Federal agency POC identified in the exclusion record.

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.

GSA requires privacy and security training for all personnel and has policies in place that governs the proper handling of PII. GSA employees receive annual security awareness training and are specifically instructed on their responsibility to protect the confidentiality of PII. All SAM system users with access to PII are required to submit to a security background check and to obtain a minimum of a background investigation.

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 owner ensure that the information is used only according to the stated practices in this PIA?

GSA requires privacy and security training for all personnel and has policies that govern the proper handling of PII. GSA has also implemented security and privacy controls for its systems. Further, OMB requires the GSA to document these privacy protections in submissions for Information Collection Requests processed under the Paperwork Reduction Act.

All GSA systems are subject to periodic audits to ensure that GSA protects and uses information appropriately. GSA takes automated precautions against overly open access controls. GSA's CloudLock tool searches all GSA documents stored on the Google Drive for certain keyword terms and removes the domain-wide sharing on these flagged documents until the information is reviewed. GSA agents can then review the flagged items to ensure no sensitive information has been accidentally placed in or inadvertently shared via these files.

[1] OMB Memorandum [*Preparing for and Responding to the 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.