Privacy Impact Assessment (PIA): OS - GDD - QTR2 - 2020 - OS629488

Date: 7/7/2020

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	OS - GDD - QTR2 - 2020 - OS629488	PIA ID:	1113146

Name of ATO Boundary:

OS - Grant-Recipient Digital Dossier

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Initiation
PTA - 1B:	Is this a FISMA-Reportable system?	Yes
PTA - 2:	Does the system include a website or online application?	Yes
PTA - 2A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	

URL Details

Type of URL	List Of URL
HHS Intranet (HHS Internal)	https://gdd-pilot.unitedsolutions.biz

PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Agency
PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 5A:	If yes, Date of Authorization	
PTA - 5B:	If no, Planned Date of ATO	5/1/2020
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	NEW

| PTA - 8: | Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions? | The Grant-Recipient Digital Dossier (GDD) is a web based tool that provides Grant Recipient risk information to Federal Agencies

The GDD collects existing Grantee information already captured in the systems described, eg, Treasury's Do Not Pay (DNP) provides information about Grant organizations excluded from doing business with the federal government. Federal Audit Clearinghouse's(FAC) maintains a public database of completed Internal Revenue Service (IRS) audits.
Payment Management System's (PMS) provides financial information (includes limited Personally identifiable information (PII) for individual/non-organizational grant recipients but not banking information),
System of Award Management SAM.gov provides the registration of businesses that work with the U.S. government.

The Function of the GDD is to display this information in a single webpage, providing an easily consumable data view in graphical format as well as logically present the information to Federal Grant professionals. |
| PTA - 9: | List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored. | GDD collects and maintains publicly information from the following sources: |

Taxpayer identification Number (TIN), which is required by Internal Revenue Service (IRS) for tax purpose.

Treasury's Do Not Pay –Treasury maintains a list of companies and organizations that they have deemed not worthy of Federal funding.

Federal Audit Clearinghouse, single audit information which maintains a public database of completed audits.

Payment Management System, provides grant payment data for example, how much federal money has been paid to a particular grant awardee at a given time.

System of Award Management SAM.gov – To do business with the federal government you must register your company with SAM. Company information is provided to the GDD.

IRS Form 990 provides required company tax information about the highest paid individuals, USA Spending provide the general public the financial status of the United States and breaks down in categories who, what and where federal dollars are being spent. Federal Awardee Performance and Integrity Information System (FAPIIS), provides the status of the health of the organization that will or is being provided Federal Grant money.

All PII is stored for 5 years.

PTA -9A:	Are user credentials used to access the system?	Yes

PTA - 9B:	Please identify the type of user credentials used to access the system.	HHS User Credentials
		
		   HHS Email Address
		
		   HHS/OpDiv PIV Card

PTA - 10:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual	The GDD accomplishes its purpose by leveraging various technologies, and the data sources discussed above, to standardize the risk evaluation data model and process, automate the collection of disparate risk-related information, display data in rapidly consumable visualizations, and facilitate the sharing of information across HHS organizational boundaries. Data includes: Grant name, Grant Recipient, Dunn and Bradstreet Numbers (DUNS), Employer Identification Number (EIN), Tax Identifier Number (TIN) . Grant financial payment history, any audits related to that specific grant i,e Single Audit. Grantee's names, email addresses, payment history, …etc., are collected from the IRS, FAPIIS, PMS, SAM.gov and shared witih the GDD to alleviate burden involved in the pre-award risk assessment process, this is done by providing all the Grant data in one easy to use source called the GDD.

PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	Yes
PTA - 10B:	Please specify which PII data elements are used.	EIN, SSN, Name, E-mail Address, Phone Numbers, Mailing Address, Taxpayer ID. *SSN are limited to only Individual Grant Recipients entities. Most all Federal Grant Recipients are organizations where no SSN is required only EIN. All SSN are masked and not shared in the GDD.
PTA - 11:	Does the system collect, maintain, use or share PII?	Yes

PIA

PIA - 1:	Indicate the type of PII that the system will collect or maintain	Truncated SSN Name Phone numbers Taxpayer ID
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Grantees
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	Above 2000
PIA - 4:	For what primary purpose is the PII used?	Employer Identification Number (EIN), SSN, Name, E-mail Address, Phone Numbers, Mailing Address, Taxpayer ID. *SSN are limited to only Individual Grant Recipients entities. Most all Federal Grant Recipients are organizations where no SSN is required only EIN. All SSN are masked and not shared in the Grant-recipient Digital Dossier (GDD). The purpose of this information is to determine the correct entity's pre award risk profile is matched to the correct grant organization.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	No secondary uses.
PIA - 6:	Describe the function of the SSN/Taxpayer ID.	Taxpayer identification Number (TIN), which is required by Internal Revenue Service (IRS) for tax purpose is used to match the correct Grant recipient. SSN is used in some cases as the Employment Identification number (EIN) that is required by the Federal Government when Issuing federal funds to grant recipients.
PIA - 6A:	Cite the legal authority to use the SSN	Debt Collection Improvement Act of 1996, 31 U.S.C. 7701(c)

PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	Social Security Number (SSN) is used as the Taxpayer Identification Number (TIN) when a grant recipient does not have a separate EIN, as allowed under tax laws, Executive Order (EO) 9397, "Numbering System for Federal Accounts Relating to Individual Persons," November 22, 1943, which states in part that "[A]ny Federal department, establishment, or agency may, whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize the Social Security Act account numbers assigned pursuant to Title 26, section 402.502 of the 1940 Supplement to the Code of Federal Regulations and pursuant to paragraph 2 of this order.
PIA - 8:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	SORN 09-90-0024 DEPARTMENT OF HEALTH AND HUMAN SERVICES 09-90-0024
PIA - 9:	Identify the sources of PII in the system	Government Sources Other HHS OPDIV Other Federal Entities
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	Not Applicable. The Grant-recipient Digital Dossier is not a direct public facing system and does not collect Personal Identifiable Information (PII) information from the general public. The information used is in established agreements between the Granting Agencies and their Grant recipient population.
PIA - 9B:	Identify the OMB information collection expiration date.	
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	The GDD uses information collected from established Federal entities. The information is collected from; System of Award Management-SAM.gov, Reference General Services Administration (GSA)'s Privacy Impact Assessment (PIA). US Department of the Treasury- reference Their PIA. Federal Audit Clearing House- Reference Census Bureau's PIA Federal Awardee Performance and Integrity Information System (FAPIIS) reference PIA.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary

PIA - 13:	Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason	The PII information is collected from the various Federal Agencies

The information is collected from; System of Award Management-SAM.gov at the General, Reference General Services Administration (GSA)'s Privacy Impact Assessment (PIA).

US Department of the Treasury- reference Their PIA.

Federal Audit Clearing House- Reference Census Bureau's PIA

Federal Awardee Performance and Integrity Information System (FAPIIS) reference the Department of the NAVY's PIA.

. If a company does not want the information to be collected by the US Federal Government, they can choose not to do business in the form of a US Federal Grant with the US Federal Government. |
| **PIA - 14:** | Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained | The PII information is collected from the various Federal Agencies sited above. If a company does not want the information to be collected by the US Federal Government, they can choose not to do business in the form of a US Federal Grant with the US Federal Government. To obtain consent please contact the source systems;

The information is collected from; System of Award Management-SAM.gov at the General, Reference General Services Administration (GSA)'s Privacy Impact Assessment (PIA).

US Department of the Treasury- reference Their PIA.

Federal Audit Clearing House- Reference Census Bureau's PIA

Federal Awardee Performance and Integrity Information System (FAPIIS) reference the Department of the NAVY's PIA. |
| **PIA - 15:** | Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not | The federal source systems that collect that information will be notified within 24 hours. |

			PII is not improperly or inadvertently modified or destroyed; The system does not allow for deletion of any records.
			Individuals who provide or modify PII cannot repudiate that action; No PII is provided within the system.
			PII is available when needed;
			PII is sufficiently accurate for the purposes needed; and
			Outdated, unnecessary, irrelevant, incoherent, and inaccurate PII is removed from the system by the originating source systems: System of Award Management-SAM.gov at the General, General Services Administration(GSA)
			US Department of the Treasury
			Federal Audit Clearing House- Census Bureau's
			Federal Awardee Performance and Integrity Information System (FAPIIS) Department of the Navy
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not		PII is reviewed for accuracy, relevancy, availability from the source systems: System of Award Management-SAM.gov at the General, General Services Administration(GSA) US Department of the Treasury Federal Audit Clearing House- Census Bureau's Federal Awardee Performance and Integrity Information System (FAPIIS) Department of the Navy The GDD Periodic review for accuracy, relevancy, usability, etc. at multiple points throughout the life cycle of the Grant and no less than annually.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access		Users
	Provide the reason of access for each of the groups identified in PIA -17		
PIA - 17A:	The PII in the form of Name, Address, EIN, etc. will be accessed by the Grant Managers of the specific federal award. No Administrators, Developers, contractors have access to PIA as the data is masked within the system.		
PIA - 18:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII		Federal Grant Professionals users will be vetted by the Granting agency. The request for access will be reviewed by the GDD System Owner or designated staff. This information is described in the GDD Memorandum of Understanding (MOU) and or GDD Service Level Agreements (SLA).

PIA - 19:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job the production system.	The Access Management System (AMS) at HHS is used to authorize individual users for access
		GDD users are approved for access by their Federal Management ensuring that these users are only allowed to access PII to expressly do their Federal Grant reviews. Request for access will be reviewed by the GDD System Owner or designated officials. The information is described in the GDD Memorandum of Understanding (MOU) and or GDD Service Level Agreements (SLA).
PIA - 20:	Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained	All developers, contractors, and users are subject to HHS' annual security training requirements.
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	Grant professionals in the Federal Awarding Agencies are provided Grants Management training by their respective Agency officials.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific NARA records retention schedule(s) and include the retention period(s)	General Records Schedule GRS 3.1: General Technology Management Records. Item 010, Information technology development project records. Temporary. Destroy 5 years after project is terminated, but longer retention is authorized if required for business use.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response	Technical security of PII maintains that all data is encrypted both at rest and in transit.
		Administrative Access to the system is controlled using HHS' proprietary Access Management System (AMS) controls accounts for which are authorized by the system owner. All user are Federally vetted through their respective Federal Agencies and Staffdivs.
		Physical Controls require a federally issued badge.
PIA - 25:	Describe the purpose of the web site, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response	The Grant-Recipient Digital Dossier (GDD) is a web based tool that provides Grant Recipient risk information to Federal Agencies.

The GDD collects existing Grantee information already captured in the systems described, eg, Treasury's Do Not Pay (DNP) provides information about Grant organizations excluded from doing business with the federal government. Federal Audit Clearinghouse's (FAC) maintains a public database of completed Internal Revenue Service (IRS) audits.
Payment Management System's (PMS) provides financial information (includes limited Personally identifiable information (PII) for individual/non-organizational grant recipients but not banking information),
System of Award Management SAM.gov provides the registration of businesses that work with the U.S. government.

The Function of the GDD is to display this information in a single webpage, providing an easily consumable data view in graphical format as well as logically present the information to Federal Grant professionals.

PIA - 26:	Does the website have a posted privacy notice?	Yes
PIA - 27:	Does the website use web measurement and customization technology?	Yes
PIA - 27A:	Select the type of website measurement and customization technologies is in use and if it is used to collect PII	Session Cookies - Does Not Collect PII
PIA - 28:	Does the website have any information or pages directed at children under the age of thirteen?	No
PIA - 28B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PIA - 29:	Does the website contain links to non-federal government websites external to HHS?	No