U.S. AGENCY FOR GLOBAL MEDIA

UNITED STATES BROADCASTING BOARD OF GOVERNORS

International Broadcasting Bureau

Technology, Services, and Innovation (TSI)

Privacy Information Enclave (PIE)

Privacy Impact Assessment

August 2021

Contact information / Approvals

System Owner: **Hal Chen**

Signature and date: Digitally signed by Windows Admin Center Encryption
Date: 2021.11.04 15:06:31 -04'00'

Information System Security Officer: **Londo Frett**

Signature and date: Londo Frett Digitally signed by Londo Frett
Date: 2021.11.05 15:36:52 -04'00'

Senior Agency Official for Privacy: **James "J.R." Reeves**

Signature and date: James L Reeves Digitally signed by James L Reeves
Date: 2022.01.03 08:21:46 -05'00'

System Overview

Provide a general description of the system. Include the purpose of the system and how it supports the Agency mission.

The hardware and software components that provide the Agency with functional and security features needed to process and store information of unusual sensitivity, such as “personally identifiable information” and other sensitive (but unclassified) information. Version 1 has been retired. Version 2 is hosted in VMware and known internally as PII (or PIE v2) (ref. diagrams).

What information is collected?

Briefly describe what information is collected for or by the system (e.g. the nature and sources of information).

For Payroll, biweekly payroll data output files from the Payroll service provider (legacy provider-State Department; current provider-DFAS) are stored in the PIE which contain Federal Employee SSN, Name, Age, Date of birth, Home address, Email address, Military service, Occupation, Grade, Step, Job title, Work address, Salary, Work history, employee benefits coverage/deductions (health, life, retirement, TSP), time and attendance data, biweekly pay/deductions, and employer benefits contributions. Also stored here are biweekly payroll data output files for Foreign Service Nationals (FSNs) working for the BBG in 26 countries from the service provider (State Department) containing similar data fields. Files stored there also include data on employee payroll indebtedness/repayments.

For Human Resources, data extracts from the Agency Human Resources system (legacy provider-USIA; current provider-DCPDS) are stored in the PIE which contain similar data elements.

For Financial system business processes, financial system data extracts are stored in the PIE related to end of tax year processes for the creation/distribution of IRS Forms 1099 to employees and vendors. The data extracts include the Name, Home Address, SSN/TIN, the Employer (BBG’s) EIN, and reportable taxable income amounts.

For Travel system business processes, travel-related data and files used in processing employee travel authorizations/vouchers and passports (Official and Diplomatic) are stored in the PIE. These files may include Passport photos, Passport/Visa applications, hand-carry letters from State Department used in visa applications, medical documents from employee physicians documenting injuries restricting the employee to specific types of travel and/or travel arrangements, scanned images of credit card receipts supporting process travel vouchers, an MS Access database used to manage the BBG's inventory of Official/Diplomatic Passports (contains data gathered from the actual passports such as Name, Passport Number, Issued Date, Expiration Date).

Related to the travel business processes, data/files pertaining to the Government Travel credit card are stored in the PIE. Files include employee applications/supporting documentation for the Government Travel credit card, reports from the servicing card provider (Citibank) on cardholder delinquencies and monthly cardholder statements (requested as part of an audit). PII data included within the files would include the cardholders name, address, SSN, Government Travel credit card account number, and card usage data.

For security operations, the Office of Security tracks investigation and clearance data, and generates reports, for contractors and employees via the Case Tracking application and website.

Is any of the information collected personally identifiable information (PII)[1]*?*
Yes.

If ***not*** *PII, the privacy impact assessment is complete. Sign and date the assessment and return to the Senior Agency Official for Privacy.*

Why Collected?

Briefly describe why the information is collected, how it supports the Agency mission, and if possible cite legal authorities for collection of the information.

The collected HR/Payroll data is used to generate documents/reports for internal/external recipients, as well as to upload payroll expense data to the BBG's financial system Momentum. Also, the data is used to respond to/support employer-related Settlement Agreements and lawsuits. Data collected on employee indebtedness is used in the collection process and processing of employee requests for waiver of repayment.

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (OMB M-07-16).

The collected data from the Momentum financial system is used to generate/provide vendors/employees with IRS Forms 1099.

Data collected for processing Official/Diplomatic Passports and travel visas is required by the State Department and embassies of the countries visited on official business for the agency. The employee medical documentation collected is required by the Federal Travel Regulations issued by GSA.

Data collected on the Government Travel credit card is required by statute and regulation in order to appropriately manage/administer the program and exercise due diligence in monitoring Government Travel credit cards for misuse.

Data collected for Case Tracking are required to support employees and contractor employment suitability determinations by the Office of Security.

Intended Information Uses

Briefly describe the intended uses of the collected information and how it is the minimum information required for the system's purpose.

The data and files being stored in the PIE are solely used for their specified purpose described in the prior section. The data collected is the minimum data required to appropriately achieve the stated goals in each of the administrative programs.

Information Sharing

Briefly describe with whom the information is shared. Include sharing both internal to the Agency as well as between the Agency and other Federal organizations and private entities.

Reports containing aggregated data required by external organization recipients (i.e. OPM, OMB, GSA, and Congress) do not include any PII data. PII data are shared with the Agency's time and attendance service provider (webTA). Data shared internally in reports does not include PII data unless a requirement of the system of record. Data shared with the auditing firm under contract with the OIG may include PII.

How Secured?

Briefly describe how the information is secured both through administrative policies and procedures as well as through technical controls implemented within the computing environment.

To access PII resources:

1. The computer must be in the proper Domain Security Group to be applied IPSec domain policy;
2. The computer must have IE v10 or newer for PII RDS/MFA access.
3. The user must have a PII domain account;
4. The user must have a phone number with either texting or voice function for the secondary factor authentication.
5. The user must be a member of proper domain group;
6. Active Directory network resources permissions (NTFS, Share, etc.) and related application restrictions are applied to the user accordingly.

Examples:

1. WSK1: IPSec policy applied. User1 has an account in PII domain, but is not any proper PII domain groups allowed to access any terminal servers. The user request is denied by RDGateway.
2. WKS2: IPSec policy applied. However, User2 has no account in PII domain. The user is not able to log onto RDS with his BROADCASTING domain account.
3. WSK3: IPSec policy applied. User3 has an account in PII domain. It is the member of a domain group allowed to access one of the terminal servers. Therefore, User3 from WSK3 is able to log onto a designated terminal server with the domain credential and a secondary authentication factor. The user still needs proper PII domain permissions to access PII resource after logon.
4. WKS4: The workstation is not the member of any IPSec security groups in BROADCASTING domain. IPSec policy is not applied on the computer. No connection is able to be established although user4 has a PII domain account, and in a proper PII domain group.

In addition:

1. IPSec is mandatory for all server communication.
2. Terminal servers are the virtual desktop of PII end users. This eliminates sensitive data from being saved on user's workstations outside PII.
3. RDS servers are the first line to block non-PII user access.
4. No end users are able to access PII servers behind the terminal servers directly.
5. The drives are encrypted on the servers where PII data stored. The user home folders are mapped onto the server by domain group policy.
6. PII domain is a separate domain from BROADCASTING as well as a separated forest of DS. No trust relation exists between them.
7. Subnet 152.75.107.0/24 is a dedicated VLAN for PII.

System of Records

Identify if this collection is a System of Records[2] as defined by the Privacy Act and requires a System of Records Notice.

System of Records Notices have been published for the various types of administrative data described in the *System overview* section by the Agency in Federal Register Vol. 69, No.148 and Vol 79, No.180.

Privacy Impact Assessment

Identify any policies, procedures, or technical controls that must be modified or implemented to mitigate risks to any PII in the system and the plan and schedule for implementing these changes.

The Agency needs to validate, if necessary improve, and document business processes that use the PIE. In addition, the PIE subdomain is a potential security weakness. The Agency has plans to migrate the PIE to a separate Active Directory forest.

[2] OMB Guidelines explain that a system of records exists only if: (1) there is an "indexing or retrieval capability using identifying particulars [that is] built into the system"; **and** (2) the agency "does, in fact, retrieve records about individuals by reference to some personal identifier.