US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/03/2016

OPDIV:

FDA

Name:

OC Telecom System Inventory

PIA Unique Identifier:

P-1801890-495198

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The Telecommunications Services Inventory (TSI)/Network Inventory and Optimization Solution (NiOS) (collectively "TSI" or "the TSI system") application is the FDA’s centralized database for information concerning ordering, paying for, and tracking telecommunications devices and services. It includes data for these expenses incurred under several different contracts, including contracts with entities such as the HHS Program Support Center (PSC) under a contract program known as the Washington Interagency Telecommunications System (WITS) 3; the General Services Administration (GSA) under its version of WITS 3; and another contract vehicle known as Networx.

TSI provides support for ordering, maintaining an inventory, and receiving invoices across these contract vehicles, for the entire life cycle of all contracts that FDA uses the system to track. TSI improves efficiency by streamlining the ordering process, ensuring Office of Management and Budget (OMB) Circular A-123 compliance, eliminating the payment of incorrect telecommunications invoices, optimizing the procurement of telecommunications services, and ensuring fiscal responsibility.

Describe the type of information the system will collect, maintain (store), or share.

TSI maintains information concerning orders FDA places, inventory of telecommunications systems, and invoices of usage and charges for lines and circuits ordered by FDA telecommunication specialists. This system tracks general inventory holdings but does not track to whom individual devices are issued (by device serial number, MAC address, global positioning system, or any other data element).

TSI maintains information such as names, work mailing address, work e-mail address and work phone numbers for FDA employees and direct contractors in their roles as authorized ordering agents and as points of contact who can assist in providing information when telecommunications lines and circuits are terminated at FDA facilities. TSI also contains the names, work mailing address, work e-mail address, and work phone as contact information for vendor points of contact as part of the receipt of authorized orders for telecommunications products and services.

TSI users are authenticated and securely access the system by employing a username and password. The system administrator provides these credentials to the user; users do not create their own usernames or passwords. All password resets are conducted by the system administrator.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

TSI is the FDA's centralized repository of telecommunications product data (orders and invoices across WITS3 PSC, WITS3 General Services Administration and Networx contract vehicles). TSI maintains records concerning all services in the telecommunications lifecycle, including information relevant to ordering, maintaining inventory and issuing invoices across all three contract vehicles.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

E-Mail Address

Mailing Address

Phone Numbers

Names, work mailing address, work phone and work e-mail address are maintained for all points of

The system maintains a username [and password] only for registered users. Only FDA employees and direct contractors can be registered users.
Logon Information (Username and Password) is for FDA employees only

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

Names, e-mail addresses, and telephone numbers may be collected for the purposes of contacting telecommunications points of contact (POCs) related to orders placed, termination of service, and/or invoice issues. The username and passwords are used for FDA employee and direct contractor access to the TSI system.

Describe the secondary uses for which the PII will be used.

None.

Identify legal authorities governing information use and disclosure specific to the system and program.

The implementation of this system is authorized by 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. In addition, the security and privacy measures for the system are required by the Federal Information Security Management Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Not applicable.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

HHS POCs can view email address of sender from an order emailed from the system.

Private Sector

Telecom carrier POCs can view email address of sender from an order emailed from the system.

Describe any agreements in place that authorizes the information sharing or disclosure.

Not applicable.

Describe the procedures for accounting for disclosures.

Not applicable.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Individuals are aware as they self-provide the PII (name, address, e-mail, telephone number) as part of registering to use the system and/or receive ordering information. FDA personnel are advised at the time of hire and are aware of the agency's use of their information in connection with agency business.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

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.

There is no opt-out process. Collection of work contact and user authentication information is necessary for sending notifications as part of the ordering process and controlling internal system access.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

If the agency changes the collection, use, or sharing of PII data in this system, the affected individuals will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a phone call or e-mail notice to the individuals.

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.

Vendor points of contact may request their names be removed or corrected at any time, for any reason, via their business relationships with FDA. Individuals who suspect their PII is inaccurate or has been inappropriately obtained, used or disclosed in any FDA system have a number of avenues available to request to rectify the situation. They may contact the FDA point of contact to notify the system owner.

Employees with such concerns can also work with their supervisors, a 24-hour technical assistance line, FDA's Systems Management Center, and other channels.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

The Standard Operating Procedure (SOP) for TSI ensures the contact information within TSI is

periodically reviewed by the TSI program manager and system administrator. These reviews include a weekly audit to report on user account events/activities (account deletion, account changes, etc.), ensuring the integrity, accuracy and relevancy of data contained in TSI. Information Integrity and availability are also protected by security controls, selected from the National Institute of Standards and Technology's Special Publication 800-53.

The Standard Operating Procedure (SOP) for TSI also ensures the contact information within TSI is periodically reviewed by the system system owner for integrity, accuracy, relevancy and availability.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

FDA employees have access to his/her own user information to take vendor orders.

Administrators:

FDA employees and direct contractors in an administrator role have access to all user information for password change/support.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

The individual user permissions limit visibility and data edit permission to his/her information only; the System Administrator has permissions to view/edit all user information.

Per FDA's standard operating procedure for activating new accounts, the TSI system administrator establishes an account in TSI for each user, assigns the user a role or roles, and associates the roles with the appropriate permissions per FDA Contracting Officers Representative (COR). The system sends the user an e-mail to the FDA e-mail address on file which has his/her user ID and a URL with text directing the user to login and immediately create a strong password. The user cannot access the system until they set up the strong password. Users have the ability to change their passwords. Any other changes are performed by the Administrator.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

System Administrator visibility and permissions are limited to those necessary to administrate the system. System administrators can, for example, view or edit user information to update or correct a user's name or e-mail address. The TSI system administrator establishes an account in TSI for each user, assigns the user a role or roles, and associates the roles with the appropriate permissions

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.

The FDA requires all Agency personnel and contractors to complete FDA's IT Security and Privacy Awareness training at least once every 12 months. A portion of this training is dedicated to guidance on recognizing and safeguarding PII.

Describe training system users receive (above and beyond general security and privacy awareness training).

Users may receive some system-specific training necessary to performing their daily duties. Additional training may be on-the-job or ad hoc, and may include additional privacy and security training.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

All records in this system are maintained under General Records Schedule (GRS) 3.2, Information Systems Security Records; Item 030, System Access Records. This schedule is for “records created

as part of the user identification and authorization process to gain access to systems." Disposition for these files is temporary, and the files may be destroyed/deleted when business use ceases. If the application owner determines that an application requires special accountability, retention may be six years after the password is altered or the user account is terminated, and longer retention is authorized if required for business use.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include usernames, passwords, use of SSL and others. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.