Privacy Impact Assessment (PIA): FDA - UCS - QTR4 - 2024 - FDA4323834

Created Date: 10/16/2024 8:23 AM Last Updated: 10/23/2024 2:22 PM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

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:	FDA - UCS - QTR4 - 2024 - FDA4323834	**PIA ID:**	2324726
Name of Component:	FDA - OC Unified Communication Services	**Name of ATO Boundary:**	OC GSS1 Network and Telecom
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	8
Submission Status:	Submitted	**Submit Date:**	10/15/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4323834
Legacy PIA ID:		**Make PIA available to Public?:**	No

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	9/7/2022
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	FDA has made no changes to this [system/component/information collection] since the last Privacy Threshold Analysis/Privacy Impact Assessment was approved.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 4:	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 Food and Drug Administration (FDA) organizes its information technology into five General Support Systems (GSS). Each of these GSS focuses on a specific theme within the Information Technology (IT) portfolio at the FDA. GSS 1 is one of these five General Support Systems that comprise the FDA's consolidated infrastructure. Unified Communication Service falls under GSS. The Unified Communication Service (UCS) is a suite of telecommunications tools. All are Cisco products. They are: 1. An instance of Unified Communications Manager version 10.x, which enables session and call control for video, voice (i.e., the FDA-wide telephone system), messaging, mobility, instant

messaging (IM), and presence (e.g., indication that a functionality is in use, such as when an individual is in attendance in a session or away from their desk). It is an integrated productivity solution that enables users to communicate from anywhere, using any device, on any network.

2. The UCS also include an instance of the Cisco Unity Connection Voice mail version 10.x, which is a voicemail and unified messaging platform. It enables the delivery of voice mail messages and voice mail management using e-mail inboxes, web browsers, Cisco's Jabber product, Cisco's Unified IP Phone, smartphones, tablets, and more. Cisco Unity Connection also provides robust speech-recognition features.

3. Cisco Unified Presence version 10.x., a tool for indicating a user's activity status within an application, including Jabber and WebEx, e.g., whether an individual is attending and logged in to a WebEx session. This information is visible to other users.

4. Cisco Jabber: Cisco Jabber™ version 10.X is a unified communications application that permits voice and video communication over the web. It is the successor application to IP Communicator 9.x, currently being phased out.

5. Cisco Emergency Responder version 10.X, a software appliance that enhances emergency calling from Cisco Unified Communications Manager. It helps assure that Cisco Unified Communications Manager sends emergency calls to the appropriate Public Safety Answering Point (PSAP, which is a call center responsible for answering calls to an emergency telephone number for police, firefighting, and ambulance services) for the caller's location, and that the PSAP can identify the caller's location and, if necessary, return the call. Cisco Emergency Responder can also notify customer security personnel of an emergency call in progress and the caller's location.

6. Cisco Enterprise License Manager is currently in production but will be upgraded to Cisco Prime License. Enterprise License Manager provides simplified, enterprise-wide management of user-based licensing, including license fulfillment. Enterprise License Manager handles licensing fulfillment, supports allocation and reconciliation of licenses across supported products, and provides enterprise-level reporting of usage and entitlement.

PTA - 5:	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.	UCS collects the following PII information: (a) first and last name; (b) work email address; (c) work phone number and; (d) biometric identifiers consisting of an individual's voice in a voicemail; (e) work mailing address; (f) user access credentials; (g) geographic location, and (h) emergency location ID numbers (ELIN). The PII data is not shared with any other system or organization. UCS collects the following non PII data: (a) type of call (regular, long distance), (b) type of device used (mobile/landline), and (c) call routing information. In accordance with the records retention schedule, the records are destroyed or deleted after 3 years or when they are no longer appropriate.
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS Username Password

PTA - 6:	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 Cisco Unified Communications System delivers fully integrated communications by enabling data, voice, and video to be transmitted over a single network infrastructure using standards-based Internet Protocol (IP). Leveraging the framework provided by Cisco IP hardware and software products, the Cisco Unified Communications System delivers unparalleled performance and capabilities to address current and emerging communications needs in the enterprise environment. The Cisco Unified Communications family of products is designed to optimize feature functionality, reduce configuration and maintenance requirements, and provide interoperability with a wide variety of other applications. Cisco's Unified Communications System (UCS), including Cisco Unity Connection 10.x, Cisco Unified Communications Manager 10.x, Cisco Unified Presence 10.x, Cisco Emergency Responder 10.x, Cisco Unified Contact Center Express 10.x, Cisco Prime License Manager 10.x; Cisco Prime Collaboration Deployment Server 10.x and IP Celerate IP Session 6.x, IP Celerate IP Studio v2.4, Uplinx v11.x is part of a unified communication suite that will provide the Food and Drug Administration (FDA) with a fully integrated multi-service, campus enterprise Voice-over-IP (VoIP) system. The system will allow client applications such as Jabber, IP Communicator, and WebEx (Rich Media) to be integrated as one. The implementation will benefit the FDA at the White Oak campus and all buildings in the metro area to provide value and a cost-effective Architecture for Voice, Video, and Integrated Data (Collaboration). Users of the system are FDA employees and Direct Contractors who are eligible to receive government issued mobile devices. Additionally, some users are also system administrators and system developers who access the system using a username and password. The username and password are generated from Active Directory and Enterprise Administrative Support Environment (EASE). Both Active Directory and EASE are covered in separate privacy assessments. The PII collected by UCS includes first and last name, professional email address, work phone number, biometric identifiers consisting of an individual's voice, work mailing address, ELINs, geographic location, and user credentials consisting of a username and password. Users of UCS use personal identifiers (name and phone number) to retrieve records held in the system.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	No

PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	
PTA - 9:	Describe the purpose of the website, 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.	
PTA - 10:	Does the website have a posted privacy notice?	
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	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?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Biometric Identifiers Mailing Address User Credentials Other - Free text Field - geographic location, and emergency location ID numbers (ELIN).
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors
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?	PII is used to facilitate routing of phone calls and voice message traffic throughout the FDA and its Public Switched Telephone Network.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The information would be used for testing system functionality during system upgrades.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	The implementation of this system, including activities such as the collection of PII necessary for operating it, are authorized by 5 U.S.C. 301, which authorizes the Secretary of HHS to create regulations necessary for meeting the missions of his or her agency. These duties are delegated to the heads of the Operating Divisions. The operation of a phone system is a basic service necessary to meet the goals and mission of all divisions of the FDA.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Users of UCS use personal identifiers (name and phone number) to retrieve records held in the system.
PIA - 8B:	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 09-90-0001, Telephone Directory/Locator System, HHS/OS/ASMB/OMAS
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Hard Copy Mail/Fax Email Online Government Sources Within the OPDIV
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No

PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	N/A. OC Unified Communication Services does not collect information from any persons other than federal employees and therefore does not require an OMB information collection approval number.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	Individuals cannot opt out of the collection of their information because submission of the PII in this system is "voluntary" as that term is understood under the Privacy Act, but required of employees to facilitate assigning users phone numbers.
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.	No such changes are planned or anticipated. If FDA changes its practices with regard to the collection or handling of PII related to UCS, the Agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include e-mail to individuals, adding or updating online notices or forms, or other available means to inform the individual.
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.	Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have several options available to resolve the situation. These individuals may contact the office or division where they have determined that their information is held. Individuals may then make further requests for their information to be corrected or amended. FDA considers these requests and, if appropriate, makes the requested changes. Employees with such concerns can additionally work with their supervisors, the Privacy Office, a 24-hour technical assistance line, FDA's Systems Management Center, and other channels. Contact information for these offices and resources is available across FDA's internet and intranet pages.

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.	An individual's PII is provided voluntarily. The individual is responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Integrity and availability are protected by security controls selected and implemented in the course of providing the system with an authorization to operate (ATO). Controls are selected based on NIST guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators Developers Contractors Others
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: Users have access to some PII to facilitate use of their phone and voicemail systems. Administrators: Employees and Direct Contractors who are administrators receive access to maintain the systems' functionality and administrative requirements. Developers: The system vendor developers may have access to PII when they provide system troubleshooting and maintenance support. Some of the developers are Direct Contractors. Contractors: Direct Contractors may serve as developers or administrators and may provide system engineering, system troubleshooting, and administrative support. Others: System vendors who are developers may require access in order to provide technical support and troubleshooting.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The FDA pays for an annual service maintenance contract which allows system developers (including Direct Contractors or vendors of proprietary or commercial off-the-shelf applications) access while being monitored by either network branch full time employees or contractors. The FDA network branch management dictates which FDA employees require access based on role.

PIA - 20:	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.	There are multiple levels of system access which can limit how much access to information an individual may have. These levels are assigned by system administrators based on role.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (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 system users at FDA take annual mandatory computer security and privacy awareness training. This training includes guidance on Federal laws, policies, and regulations relating to privacy and data confidentiality, integrity and availability, as well as the handling of data (including any special restrictions on data use and/or disclosure). The FDA Office of Digital Transformation (ODT) verifies that training has been successfully completed.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	No additional system-specific training is received by users; however, users are provided with user guides and manuals and privacy guidance is available on the FDA intranet and from Privacy staff.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	The records and PII in UCS is maintained under FDA File Code FDA-9661 and National Archives and Records Administration (NARA) General Records Schedule (GRS) 5.5 item 10 (Mail, Printing, Telecommunication Services, Administrative & Operational Records) The disposition is temporary, the records are destroyed or deleted after 3 years or when they are no longer appropriate.
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.	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 use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at 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.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	10/16/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	The FDA's Senior Official for Privacy (SOP) has: (a) approved the Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) conducted for the subject system/component; (b) reviewed and approved the associated security categorization; and (c) reviewed and confirmed acceptable implementation status of the assigned privacy controls.	**SOP Review Date:**	10/16/2024
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	10/16/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 10/16/2024 comments have been address, this PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	0

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	10/23/2024
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
OC Unified Communication Services_SOP Approved.rtf	772494	.rtf	10/17/2024 8:36 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	VILLAFUERTE, NESTOR	10/16/2024	Please include all of the PIA elements mentioned in the PTA (ELIN, geographic locations)	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	10/23/2024 2:22 PM	**History Log:**	View History Log