Date of Approval: **June 16, 2021**

PIA ID Number: **5947**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

GSS-15 Contact Center, GSS-15

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Contact Center GSS-15 - 3243

What is the approval date of the most recent PCLIA?

5/16/2018

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

IT User and Network Services (UNS)

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

Yes

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

GSS-15 supports the IRS business in responding to taxpayer requests and services in an expedient and efficient manner and represents one of the largest and most complex Contact Center Environment (CCE) in the world. GSS-15 components are dispersed throughout IRS facilities nationwide, including over 26 call center sites, and supports over 15,000 customer service representatives (CSRs). GSS-15 provides an efficient, cost effective, secure and highly reliable contact center infrastructure and voice network for IRS business entities and taxpayers using the CCE. GSS-15 contains the voice network and telecommunications equipment that supports the CCE, which contains several business unit applications such as Wage and Investment (W&I), Small Business Self-Employed (SBSE), and Electronic Products and Services (EPPS). Infrastructure and applications within GSS-15 boundary are primarily managed by the Contact Center Support Division (CCSD) within UNS (User Network Services) and by Enterprise Operations (EOPS). W&I is primarily responsible for managing and maintaining their applications such as Integrated Data Retrieval System (IDRS) and eWorkforce Management (eWFM). CCSD is responsible for managing the systems and applications used to monitor, manage, and maintain the critical telephony infrastructure that encompasses components of the CCE. To ensure effective operations, GSS-15 uses state of the art call routing and distribution equipment. CCSD is responsible for managing the day-to-day operations of the CCE and is the integrator of technical and program services for the successful delivery of IT commitments to the business. GSS-15 provides real time monitoring and scripting as well as operational support to ensure all contact center technology is functioning and meeting business requirements.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e. last 4 digits, etc.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

When there is no reasonable alternative means for meeting business requirements.

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

The Contact Recording (CR) and Contact Analytics (CA) systems do not use Social Security Numbers (SSNs). The CR system records the spoken conversation between taxpayer and agent. Any spoken SBU/PII data is retained in the audio recording. The CR system also records the workstation interactions via a video recording. Any SBU/PII pulled up on the agent's workstation will be captured in the video recording. CA is used to evaluate the audio of taxpayer calls that were recorded using the Contact Recording system. The analysis results are used to identify Contact Center improvement activities that will enhance quality and reduce operations costs. Predictive Dialer System (PDS) - The Business Compliance organization currently use the Dialer for more efficient call outreach, reducing agent resources in approximately 3.9 million collection cases. The taxpayer file data elements as defined by the agency are imported into a custom flat file. This fixed-width Import file is used by the application to create outbound call campaigns. Actual SSNs are not directly utilized but are associated with the Customer Reference Numbers for authentication. Customer Contact Voice Response Unit (CC-VRU) - CC-VRU provides taxpayers with automated information about refunds, office locations, refund transcripts, payoffs, and collections. The CC-VRU system collects SSN on the primary taxpayer and spouse. SBU/PII data is used for transaction handling for troubleshooting purposes and exists within CC-VRU log files until overwritten.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

Contact Recording (CR) and Contact Analytics (CA) - The CR system only records the audio and screen captures from the other IRS systems. The information contained in the recordings is controlled by the contents on the systems used on the agent's workstation. The CR and CA software cannot make any changes to the files once recorded. Any steps to mitigate or eliminate the use of Social Security Numbers (SSN's) would have to come from the other IRS systems that appear on the agent's computer screen. Predictive Dialer System (PDS) - Currently no mitigation strategies are implemented to eliminate the use of TINs (Taxpayer Identification Numbers). Mitigation techniques would invalidate application ability to update and validate customer interactions. Customer Contact Voice Response Unit (CC-VRU) - Currently, there is no plan to eliminate the use of SBU/PII data in CC-VRU because it allows tracking of transactions for troubleshooting purposes and only exists temporarily within CC-VRU log files and is overwritten constantly. Also, to suppress CC-VRU SBU/PII information, a code change will be required by the vendor.

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name
Mailing address
Phone Numbers
E-mail Address
Standard Employee Identifier (SEID)
Biometric Identifiers
Employment Information
Tax Account Information
Centralized Authorization File (CAF)

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant).

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

All components of the Contact Center use PII data for authentication and security purposes - Intelligent Contact Manager (ICM), Customer Voice Portal (CVP), Active Directory (AD), Aceyus, Contact Recording (CR), Contact Analytics (CA), The Infrastructure Upgrade Project - Endpoint Replacement (IUP-ER)/UCCE, E-Workforce Management (eWFM), Teletypewriter/Telecommunication Devices for the Deaf (TTY/TDD), Predictive Dialer System (PDS), Customer Contact Voice Response Unit (CC-VRU). In addition, the PDS, CC-VRU, CR/CA components use SBU data. PDS - The Business Compliance organization currently use the Dialer for efficient out-dial call campaigns for tax collection. The Taxpayer data elements as defined by the agency are required in order to sort the data into a campaign type and ensures the correct taxpayer record is updated with date, time, and total number of attempts to contact the taxpayer. A Customer Reference Number (which acts as an alias for taxpayer's SSN) is used to validate the taxpayer contact with agent's screen data. Customer Contact Voice Response Unit (CC-VRU) - CC-VRU provides taxpayers with automated information about refunds and collections. The CC-VRU system collects SSN on the primary taxpayer and spouse. SBU/PII data is used to track transactions for troubleshooting purposes and exists within CC-VRU log files until overwritten. CR and CA - The primary purpose is for quality. The information is collected for Centralized Quality Review System (CQRS). CQRS can evaluate whether the assistor gave the taxpayer a correct answer or not. In order to assist taxpayers, assistors must be able to verify disclosure to access their tax information. This is done by accessing the information and accounts via the taxpayer's SSN.

How is the SBU/PII verified for accuracy, timeliness and completion?

Predictive Dialer System (PDS) - The PDS system uses a custom Customer Reference Number that acts as an alias for the taxpayer information, which includes all Taxpayer data elements as defined by the agency (i.e., Taxpayer name, address, phone, SSN, etc.). Customer Contact Voice Response Unit (CC-VRU) - CC-VRU log files capture only the taxpayer's input. Therefore, if the SBU/PII information the taxpayer enters is inaccurate, the log files will be inaccurate. Also, if the taxpayer enters incorrect information after a set number of times, he/she will be re-prompted to enter the information again or be transferred to an agent. Contact Recording (CR), Contact Analytics (CA) - The CR system only records the audio and screen captures from other IRS systems. The CR and CA software cannot make any changes to the files once recorded. Any verification would have to come from the other systems that appear on the assistor's computer screen.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 34.037 Audit Trail and Security Records

IRS 00.001 Correspondence Files and Correspondence Control Files

IRS 26.019 Taxpayer Delinquent Account Files

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 36.003 General Personnel and Payroll Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Integrated Data Retrieval System
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: Yes
ATO/IATO Date: 10/14/2020

System Name: OnLine 5081 (OL5081)
Current PCLIA: Yes
Approval Date: 9/13/2018
SA&A: Yes
ATO/IATO Date: 2/28/2020

System Name: Corporate Authoritative Directory Service (CADS) - GSS-17
Current PCLIA: Yes
Approval Date: 9/18/2020
SA&A: Yes
ATO/IATO Date: 10/30/2019

System Name: Automated Collection System (ACS)
Current PCLIA: Yes
Approval Date: 10/12/2018
SA&A: Yes
ATO/IATO Date: 11/20/2020

System Name: IBM Security and Communication Platform (SACS) - GSS-21
Current PCLIA: Yes
Approval Date: 9/15/2018
SA&A: Yes
ATO/IATO Date: 9/17/2020

System Name: ICCE
Current PCLIA: Yes
Approval Date: 5/29/2019
SA&A: Yes
ATO/IATO Date: 6/27/2021

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 433-F
Form Name: Collection/Information Statement

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Splunk
Current PCLIA: Yes
Approval Date: 1/27/2020
SA&A: Yes
ATO/IATO Date: 3/28/2017

System Name: Automated Collection System (ACS)
Current PCLIA: Yes
Approval Date: 10/12/2018
SA&A: Yes
ATO/IATO Date: 11/20/2020

Identify the authority.

IT Enterprise Operations (EOPS)

For what purpose?

Predictive Dialer System (PDS): The Business Organizations Small Business/Self Employed (SBSE), Wage and Investment (W&I) and Compliance currently use the Dialer for efficient call management. The purpose of the calls to the taxpayer is to reduce the approximately 3.9 million collection cases. The Taxpayer file data elements as defined by the agency are required in order to sort the data into a campaign type and ensuring the correct taxpayer record is updated with date, time, and total number of attempts to contact the taxpayer. In order to verify that the correct taxpayer has been contacted, the taxpayer screen data is required. The taxpayer file data elements are required in order to sort the data into a campaign type.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

Yes

Briefly explain how the system uses the referenced technology.

Contact Recording is a part of GSS-15 and it records a call between an IRS agent and taxpayer capturing voice biometrics.

Does the system use cloud computing?

No

Does this system/application interact with the public?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Not Applicable

Please explain.

The Customer Contact - Voice Response Unit (CC-VRU) is a self-service enterprise environment that provides a transparent response system to taxpayers calling to obtain information that can be supplied without needing to speak to a customer service agent. CC-VRU provides infrastructure support for a suite of telephony and web applications that are within the boundary of the Integrated Customer Communications Environment (ICCE) application. The ICM/CVP systems route calls to the CC-VRU system. Taxpayers use the automated menu system on CC-VRU to indicate what information they seek. Based on the taxpayer's menu selection, the CC-VRU software then routes these calls to the appropriate ICCE application for access to automated information or to the Customer Voice Portal (CVP) environment for access to a live agent via the Cisco unity call manager. The CC-VRU call response hardware and software are the only portion of this automated system that reside in the GSS-15 boundary. The phone applications are managed under the ICCE authorization boundary.

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

CR: Taxpayers are notified via a recorded announcement that the call may be recorded, prior to being connected to an agent. Notice, Consent and Due Process are provided pursuant to 5 USC.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

CR: In the event a taxpayer doesn't want a call to be recorded between he/she and an agent, the agent can stop the recording via a button on their computer keyboard. Notice, Consent and Due Process are provided pursuant to 5 USC.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

IRS policy allows affected parties the opportunity to clarify or dispute negative determinations per the examination appeals process as outlined in IRS Publication 1 - Your Rights as a Taxpayer, and IRS Publication 5 - Your Appeal Rights and How To Prepare a Protest If You Don't Agree. Notice, Consent and Due Process are provided pursuant to 5 USC.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated).

IRS Owned and Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Only

Managers: Read Only

System Administrators: Administrator

Developers: Read Write

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Administrator

Contractor Developers: Read Write

How is access to SBU/PII determined and by whom?

Account access is managed through the Online 5081 process. Appropriate approvals at several levels are required to grant access to components within GSS-15.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

GSS-15 General Support System (GSS) is non-recordkeeping and does not require National Archives and Records Administration approval for records disposition or retention. GSS-15 contains the voice network and telecommunications infrastructure that supports the Contact Center Environment (CCE). As described below, the IRS applications that GSS-15 supports have their own approved retention standards and recordkeeping requirements. Predictive Dialer System (PDS): When file processing has completed, the original fixed-width file delivered by the agency is written to a temporary location for archival, troubleshooting purposes, and purging. CA/CR: Follows Records Control Schedule (RCS) 31 for Customer Service, item 24. GSS-15 Audit logs are maintained in accordance with General Records Schedule (GRS) 20, Item 1c. For IRS systems that store or process taxpayer information, audit trail archival logs are retained for 7 years, unless otherwise specified by a formal Records Control Schedule developed in accordance with Records Management. At the end of the standard maintenance period, the audit logs are reviewed to determine if the logs require additional retention to support administrative, legal, audit, or other operational purposes, or if destruction is appropriate. Further guidance for the capture and retention of audit-related records is found in IRM 1.15 and IRM 10.8.1 Security - Policy and Guidance.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

6/17/2020

Describe the system's audit trail.

ICM, CVP, Active Directory (AD), Aceyus, IUP: Only employee data (SEID) is contained within audit logs. An employee SEID is captured when there is a failed login attempt. CC-VRU: The security audit system tracks elements such as login ID, login date/time, logout date/time, files/directories accessed, attempted security violations, Data from system audit and monitoring files are used to measure system performance including availability, reliability, usability, and resource usage. Additional audit trail data is captured to monitor system access at the operating system level. This security audit data is gathered by the commercial-off-the-shelf (COTS) security auditing capability provided with the operating system. Data gathered by the security audit system includes login ID, login date/time, logout date/time, files/directories accessed, attempted security violations, and administrative actions. Access to and maintenance of security audit data is described in trusted facility manuals for the CC-VRU. Predictive Dialer System (PDS): The system is secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements. Data gathered by the security audit system includes login ID, login date/time, logout date/time, files/directories accessed, and attempted security violations. CA/CR: Data gathered by the security audit system include taxpayer's name, SSN, phone number, Employer Identification Number (EIN) and address. eWFM: The OS documents user login information and their associated actions, however a detailed transaction log is not maintained for the system. TTY: The following application user information is stored within the system: Username, first name, last name and location.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

Treasury FISMA Inventory Management System (TFIMS)

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

GSS-15 components undergo an Annual Security Control Assessment (ASCA) and Information Security Contingency Plan exercise every year. These initiatives are conducted by Cybersecurity. Cybersecurity develops the test plans, assess the systems, document the results and deliver a final package to GSS-15 Stakeholders for information and action. All identified security risks are entered into the Treasury FISMA Inventory Management System (TFIMS) as Plan of Action and Milestones (POA&M). These items are updated and closed on or before their scheduled completion dates.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Under 50,000

Contractors: Under 5,000

Members of the Public: 100,000 to 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

Yes

Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

Per IRM 10.8.1 Security - Policy and Guidance, all GSS-15 components have auditing enabled at the operating system level which captures system, application and security related information. The audit records are sent to Cybersecurity on a routine basis and thus retained based on IRS retention guidelines. In order to access the audit trails once the files have been sent to Cybersecurity, GSS-15 System Administrators have to complete an OL5081 request, which has to be approved by management in CCSD and Cybersecurity.

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent?

No