Date of Approval: May 16, 2018 PIA ID Number: **3243**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Contact Center, GSS-15

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Contact Center, GSS-15 1300

Next, enter the **date** of the most recent PIA. 4/16/2015

Indicate which of the following changes occurred to require this update (check all that apply).

No	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
No	Significant Merging with Another System
No	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
No	New Interagency Use
No	Internal Flow or Collection

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
No	System Development/Milestone 4B
No	System Deployment/Milestone 5
Yes	Operations & Maintenance (i.e., system is currently operational)

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

A.1 General Business Purpose

5. 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.

General Support System (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 Contact Center Environment (CCE). GSS-15 contains the voice network and telecommunications infrastructure that supports the CCE, which contains several Wage and Investment (W&I) business unit applications. Infrastructure and applications within the boundary of GSS-15 are primarily managed by the Contact Center Support Division (CCSD) within UNS (User Network Services) and by Enterprise Operations (EOPS). W&I has the primary responsibility to manage and maintain their applications. CCSD is responsible for managing the systems and applications which are used to monitor, manage, and maintain the critical telephony infrastructure that encompasses components in the CCE. Additionally, CCSD is responsible for managing the day-to-day operations of the CCE. The CCE supports the IRS's 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 environments 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).

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse Yes On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes Social Security Number (SSN)
Yes Employer Identification Number (EIN)
Yes Individual Taxpayer Identification Number (ITIN)
Yes Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes Practitioner Tax Identification Number (PTIN)

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

Contact Analytics (CA) and Contact Recording (CR) do not use the Social Security Number (SSN), Employer Identification Number (EIN), Individual Taxpayer Identification Number (ITIN), Adoption Taxpayer Identification Number (ATIN) or Preparer Tax Identification Number (PTIN) as an identifier within the system. This information is not a data field maintained by either component. As such, there are no planned mitigation strategies or forecasted implementation dates to mitigate or eliminate the use of Social Security Number (SSN)s on GSS-15 components as this information is received from the Integrated Data Retrieval System (IDRS). 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 to ensure that the correct taxpayer record is updated with the date, time, and total number of attempts to contact the taxpayer. The IRS PDS Import Service provides a Microsoft Windows based Service Application that accepts the fixed width import file containing dialing information for the contact center. This fixed-width Import file is re-named with a unique name and converted to a comma delimited file that can be accepted and read by the icList software to create call campaigns. Currently no mitigation strategies are implemented to eliminate the use of TINs (Taxpayer Identification Numbers). Mitigation techniques are used to remove files with PII including file purging processes setup for removing the fixed width import file containing dialing information. Customer Contact Voice Response Unit (CC-VRU) collects SSN on the primary taxpayer and spouse. There are 2 logs that capture PII in the Voice Browsers: 1) History logs - generated by Integrated Customer Communications Environment (ICCE) Telephone applications and 2) Voice Extensible Markup Language (VXML) logs - generated by Convergys' Commercial Off-The-Shelf Software (COTS) when TIN is spoken. A change to ICCE code in the Voice Browser will be necessary to suppress PII from History logs. This will make troubleshooting a problem originated on the Telecommunication side significantly more difficult since it will be harder to correlate Presentation Web Application Server (PWAS) transaction information to Voice Browser's. We will have to rely on the time stamp & channel number. For PII to be suppressed in VXML logs, Convergys will need to be engaged to make sure that is done properly and without impact to voice applications.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
Yes	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	Yes

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
No	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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.

Intelligent Contact Manager (ICM), Customer Voice Portal (CVP), Active Directory, Automated Call Distributor (ACD), ACD-Proxy and ACD- Unified Command and Control Real Time Reporting (UCC-RTR): The user's Standard Employee Identifier (SEID) is required for security purposes. CC-VRU: CC-VRU: CC-VRU serves as the data access bridge between the Integrated Data Retrieval System (IDRS) (via Security and Communications System (SACS)) and the Web Servers and Voice Response Units. SBU/PII data allows tracking of transactions for troubleshooting purposes and only exists temporarily within CC-VRU log files and is overwritten constantly. ACD: The SEID

is required so management can determine which employee is associated with a extension/user record. 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 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. To verify that the correct taxpayer has been contacted, the taxpayer screen data is required. The taxpayer file data elements are required to sort the data into a campaign type. E-Workforce Management (eWFM): The user's SEID is captured for user identification purposes within the database. Teletypewriter/Telecommunication Devices for the Deaf (TTY/TDD): This information is collected to determine application access.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

Intelligent Contact Manager (ICM), Customer Voice Portal (CVP), Active Directory, Automated Call Distributor (ACD), ACD-Proxy, and ACD- Unified Command and Control Real Time Reporting (UCC-RTR): Time stamps are attached to each data item and Cybersecurity reviews logs for consistency. Customer Contact – Voice Response Unit (CC-VRU): Data elements are not part of the CC VRU infrastructure. ACD: Employee information within the system is based on when an employee is hired and then when terminated or in non-duty status. Predictive Dialer System (PDS): The PDS system receives the daily fixed width import file containing dialing information. Once received the import processing service loops through every row in the fixed length file, executes any necessary data transformation and converts the row to comma-delimited text. It then determines whether records are valid or invalid and writes a record to the main campaign file and/or the bad records campaign file. If the record is valid then only a record in the main campaign file will be generated. If the record is invalid then only a record in the bad records campaign file will be generated. If there is a mix of both valid and invalid content in the incoming record, then 2 records will be generated, one for the bad records campaign and one for the main campaign. Only valid records will be included in the main campaign row and invalid records will be included only in the bad records campaign record. There should be no invalid records written to the main campaign file and no valid content written to the bad records campaign file. The main campaign file and the bad records campaign file will be written by the service to the directory that icList is expecting the files to arrive at. When file processing has completed, the original fixed-width file delivered by the agency will be written to a temporary location for archival, troubleshooting purposes, and purging. Contact Analytics/Contact Recordings (CA)/CR): The CA application will interface with the master recording index maintained by the CR system that stores information on the location of recorded conversations by agent, call type, handle time, and other metadata. E-Workforce Management (eWFM): Data is updated continually by site staff as employee schedules change (i.e. sick leave) and training level changes. The overall database (employee schedules being tracked) is verified and cleaned up quarterly. Teletypewriter/Telecommunication Devices for the Deaf (TTY/TDD): Only application user information is stored within the system. This is used to track information within the database. This information is not verified for accuracy, timeliness, or completeness.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	SORNS Name
IRS 34.037	Audit Trail and Security Records System
IRS 34.016	Security Clearance Files
IRS 00.001	Correspondence Files and Correspondence Control Files
IRS 26.019	Taxpayers Delinquent Accounts Files
IRS 24.030	Customer Account Data Engine Individual Master File
IRS 24.046	Customer Account Data Engine Business Master File

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Integrated Data Retrieval System	Yes	10/17/2016	Yes	11/08/2016
Automated Collection System (ACS)	Yes	10/17/2016	Yes	11/08/2016
IBM Security and Communication Platform (SACS)	Yes	10/22/2015	Yes	02/16/2016
ICCE	Yes	03/30/2016	Yes	07/03/2017

11b. Does the system receive SBU/PII from other federal agency or agencies? No

11c. Does the system receive SBU/PII from State or local agencies? No

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

Form Number	Form Name
433-F	Collection/Information Statement

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

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

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide 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.

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

18a. If **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.

19. 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.

I. INFORMATION PROTECTION

20. 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

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

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Administrator
Developers	Yes	Read and Write

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read-Only	Moderate
Contractor Managers	Yes	Read-Only	Moderate
Contractor Sys. Admin.	Yes	Administrator	High
Contractor Developers	Yes	Read and Write	Moderate

21a. 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.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22a. If **yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and 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.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 7/12/2017

23.1 Describe in detail the system s audit trail. ICM, CVP, Active Directory: 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. ACD, ACD-Proxy, and ACD-UCC-RTR: The audit trail does not contain any employee information or PII. A manager can request a report which contains call statistics by login, which includes the employee's name. Eventually the SEID will be captured within the event logs. 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process,** 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.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? All GSS-15 security and applicable test plan documentation is stored on CCSD SharePoint site.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Under 50,000
26b. Contractors: Under 5,000
26c. Members of the Public: More than 1,000,000
26d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

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

If **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.

N. ACCOUNTING OF DISCLOSURES

30. 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

End of Report