Date of Approval: **November 09, 2022**

PIA ID Number: **7327**

SYSTEM DESCRIPTION

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

Finesse, Finesse

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?

FINESSE. PCLIA # 6789

What is the approval date of the most recent PCLIA?

3/17/2022

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

Were there other system changes not listed above?

Yes

What were those changes?

Additional system functionality is being included and infrastructure capacity is being expanded. None of these changes impact the type of data that the system processes. In addition, a Gadget (navigational link) to an external cloud-based eGain Chat service is being added to Finesse. eGain chat service is a GovCloud Software as a Service (SaaS) application that has been in used at the IRS since about 2019. The eGain Chat service privacy is addressed by PCLIA # 5188. In addition, a Gadet (navigational link) to another application is being added to Finesse. The application is the Acqueon List and Campaign Management (LCM) which is part of the same General Support System15 as Finesse. The LCM application may display PII such as TIN, telephone #, or Taxpayer name. The LCM application privacy is addressed PCLIA # 5947.

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

Technical Integration Governance Board (TIB)

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

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.

The Internal Revenue Service (IRS) Contact Center Support Division (CCSD) manages and operates the Information Technology (IT) infrastructure that supports the Taxpayers, the Enterprise Service Desk (ESD), and the Enterprise Resource Center (ERC) contact centers. The Taxpayers contact center is used by taxpayers to ask questions pertaining to tax matters, or questions related to specific tax cases. The Taxpayers contact center is also used by the IRS for dial-out campaigns related to collection matters. The ESD and ERC contact centers are used by IRS employees. IRS employees contact the ESD with questions related to IT problems/issues, and they contact the ERC with questions related to benefits or general Human Resources related questions. The Contact Center currently uses Cisco's Computer Telephony Integration Operating System (CTIOS) and IP Blue computer applications to provide Agent/Supervisor Desktop functionality. CTIOS is out of manufacturer support and will no longer be supported as the IRS transitions its contract center infrastructure to the manufacturer recommended architecture. CTIOS/IP Blue will be replaced with Cisco Finesse (the system). Finesse will provide the same Agent/Supervisor Desktop functionality as CTIOS/IP Blue - that is, call management functions and agent monitoring functions. Finesse is essentially a soft phone without a voice stream with some additional features that allows supervisors to monitor Agents' state. Finesse is a pass-through system that does not store any records or PII information. The main benefits to the IRS from the system is that instead of two Agent/Supervisor Desktop applications to maintain, there will only be one, thus, there will be significant maintenance, support, and enhancements cost reductions. In addition, because Finesse is a World Wide Web (Web) browser-based application, unlike CTIOS/IP Blue that are both applications installed in a contact center agent's computer, the process of deploying the system and enhancement to contact center sites will be simplified resulting in the reduction of time and costs to push out new functionality to contact center sites.

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:

Interfaces with external entities that require the SSN

When there is no reasonable alternative means for meeting business requirements

Delivery of governmental benefits, privileges, and services

Another compelling reason for collecting the SSN

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

The system itself does not collect SSN. The SSN is captured by another system (Interactive Voice Response (IVR) unit) and is passed onto the system for display to a contact center agent which uses it to retrieve information pertinent to the caller.

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

There is no plan to eliminate the use of SSNs. The Office of Management and Budget memorandum Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record.

Employer 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
Phone Numbers
Standard Employee Identifier (SEID)
Internet Protocol Address (IP Address)
Tax Account Information

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

No

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

Yes

Describe the other types of SBU/PII that are applicable to this system.

System level information includes user id's, case id's, activity id's, log files, command codes, activity dates, activity types which could be considered SBU.

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.

The SSN number is used by contact center agent to pull a taxpayer's records when the taxpayer calls the IRS. The call center Agent's name and SEID (PII) are used for purpose of supervisors monitoring agent state and logging off the agent from the system. The Agent's SEID is also used for logging into the system.

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

The system of record is the functional system that is responsible for the accuracy of the PII. When PII is transmitted to the system the confidentiality and integrity of the data will be protected. The contact center agent may also verify the accuracy of the customer's PII with the customers over the phone.

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 00.001	Correspondence Files and Correspondence Control Files
IRS 34.037	Audit Trail and Security 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: Contact Center, GSS-15
Current PCLIA: Yes
Approval Date: 6/16/2021
SA&A: Yes
ATO/IATO Date: 4/28/2021

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?

No

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

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

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.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

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?

All callers are notified prior to being connected to an agent that their call may be recorded or monitored. Notification is via the Customer Voice Portal (CVP) system.

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):

The caller may request their call not be recorded via the agent. The agent will stop the recording at that point.

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

Notice, Consent and Due Process are provided pursuant to 5 United States Code (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 System Administrators: Read Write

Contractor Developers: Read Write

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

Account access is managed through the Business Entitlement Access Request System (BEARS) process. Appropriate approvals at several levels are required to grant access to the system.

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?

No

You must work with the IRS Records and Information Management (RIM) Program Office to address records retention requirements before you dispose of any records in this system.

SA&A OR ASCA

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

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

The system is an integral subcomponent of the Intelligent Contact Management (ICM). The system does not and cannot stand alone. A user uses the system to login into the ICM - The system itself does not store login information. The ICM security audit system tracks elements such as login ID, login date/time, logout date/time, files/directories accessed, attempted security violations, Data from ICM 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 ICM 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.

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)?

Test results are stored in Collaborative Lifecycle Management (CLM) tool, a web-based tool to manage requirements, development/implementation, and QA/testing in an integrated way. This tool is mandated by the Enterprise Lifecycle (ELC) Program Office for all project that follow the Agile ELC Path. This is a tool that provides traceability from requirements, through development/implementation, and testing.

Were all the Privacy Requirements successfully tested?

No

Please explain which Privacy Requirements were not tested and why?

Not all testing has been completed yet. The project follows the ELC Agile path in which functionality is built and tested incrementally. The project is still in the development stages (ELC Agile Milestones IRR). The testing will address Privacy Requirements as appropriate.

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?

No all testing has been completed. Access controls and encryption will be assessed for PII and tested if it is not an inherent control.

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: Not Applicable

Contractors: Not Applicable

Members of the Public: Not Applicable

Other: Yes

Identify the category of records and the number of corresponding records (to the nearest 10,000).

The Finesse system is essentially a phone control application. The only information it captures, and stores is system events (e.g., who logged into the system, error messages, authentication errors, etc.) These system logs are sent to Cybersecurity and are processed by the Cybersecurity Streaming Data Monitoring Tool (aka Splunk). These records will number in the thousands/day (over 171 MB of data per day is anticipated).

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?

No

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