Date of Approval: **October 27, 2022**

PIA ID Number: **7310**

SYSTEM DESCRIPTION

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

Beyond Trust Remote Support Appliance Tool, Beyond Trust

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?

Bomgar, PIA # 4376

What is the approval date of the most recent PCLIA?

10/17/2016

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.

User and Network Services (UNS) Governance Board

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?

No

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 Customer Service Support (CSS) organization and the Enterprise Field Operations (EFO) organization provide support to customers within the IRS. The Beyond Trust Remote Support Appliance software gives support technicians secure remote control of computers, over the Internet or on local networks. This specialized appliance provides exceptional performance, reliability, ease of use and scalability through a solution that is optimized for remote support. It will be deployed throughout the Enterprise. This software is a comprehensive remote support solution that will satisfy mandates from the Office of Management and Budget (OMB), Treasury, Department of Homeland Security, and the White House relative to the SmartCard Compliance Directive. This software aligns with the current appliance-based architecture and will be deployed using IRS software deployment tools. With the implementation of this software, UNS support technicians in CSS/ Enterprise Service Desk (ESD) and EFO will have the ability to remotely support customers following mandated requirements and in a secure environment.

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.)?

No

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
E-mail Address

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?

No

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

PII for personnel administration is 5 USC

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.

When an IRS employee contacts the IT Service Desk for assistance the IRS employee provides their name, SEID, contact phone number and is requested to verify their office address. This information is entered into the Knowledge Incident/ Problem Service and Asset Management (KISAM) / IRWorks system to create an incident or interaction with a detailed description of their computer related issue/problem. Beyond Trust software maybe used to remote into the IRS employee's computer to resolve the issue.

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

The information is verified by the IRS employee upon contact with the IT Service Desk for assistance.

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 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?

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?

This is an internal use system only. IRS Employees contact the help desk and provide information such as name and SEID. Notice, consent, and due process is generally provided during KISAM logon.

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):

This is an internal use system only. IRS Employees contact the help desk and provide information such as name and SEID. Notice, consent, and due process is generally provided during KISAM logon.

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

This is an internal use system only. IRS Employees contact the help desk and provide information such as name and SEID. Notice, consent, and due process is generally provided during KISAM logon.

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 Write

Managers: Read Write

System Administrators: Administrator

Developers: Read Write

IRS Contractor Employees

Contractor Users: Read Write

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

Access is based on an approved BEARS. A potential user will request access via the BEARS system. This request has to be approved by the potential user's manager based on a user's position and need-to-know. Contractors with IRS laptops would be covered, and they would have Staff-Like access using IRS Laptops/equipment. The contractor background investigation level and access permissions may vary depending on contract requirements but the moderate clearance to obtain an IRS laptop will be authorized.

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.

Beyond Trust is an interaction utility to be used in conjunction with KISAM / IRWorks. All IT help desk interaction records are properly scheduled under the Record Control Schedule of the IRS, (RCS) 17 for Information Technology, Item 23(b)(2); and The General Record Schedules (GRS) 5.8 Administrative Helpdesk Records, Item 010. For Beyond Trust, audit trails, user accesses and logins are all scheduled in GRS 3.2 for Information System Security Records, Item 030. All data housed in Beyond Trust will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6.

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?

Do not know

Describe the system's audit trail.

Session data is automatically captured by the Bomgar software and is uploaded into KISAM / IRWorks interaction incident. Beyond Trust is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

Beyond Trust is currently being used in the IRS environment and not required. Beyond Trust is in FISMA Non-Reportable Status. Where this is a minor tool and not FISMA reportable, a test plan is not required. However, informal testing is conducted including functionality testing against business requirements via KISAM / IRWorks.

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: 50,000 to 100,000

Contractors: Under 5,000

Members of the Public: Not Applicable

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?

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