Date of Approval: **December 14, 2020**

PIA ID Number: **5593**

SYSTEM DESCRIPTION

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

Wireless Solutions (WS) Smartphone Devices, WSSD

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?

Bring Your Own Device (BYOD) - Good for Enterprise, BYOD, PCLIA 1358

What is the approval date of the most recent PCLIA?

11/8/2017

Changes that occurred to require this update:

New Access by IRS employees or Members of the Public

Expiring PCLIA

Were there other system changes not listed above?

Yes

What were those changes?

User and Network Services (UNS) Wireless Solution will merge both Government Furnished Devices (GFD) and Bring your own devices (BYOD) PIA's since they both utilize the same system and technology. The following technologies are currently being used for mobile solutions and comply to the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 validated encryption. They include, Artifex Software, Blackberry Corporation, BlackBerry Limited, Blackberry LLC, Branchfire, Inc., Byte Squared, Good iWare, Inc, Good Technology, Infraware Co. Ltd., Inkscreen LLC, Splashtop Inc, Zoom Video Communications.

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

NA

Current ELC (Enterprise Life Cycle) Milestones:

Preliminary Design/Milestone 3

Detailed Design/Milestone 4A

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.

BlackBerry Unified Endpoint Management (UEM) a server-based solution that supports the direct management of apps in a single console. UEM gives IT a single solution to secure and manage mobiles devices, remotely control, change and secure mobile devices. It also allows for tracking, managing, and securing Government Furnished Device (GFD) or Bring your own Device (BYOD). The "Bring Your Own Device" (BYOD) program to permit IRS personnel to use non-government furnished/personally owned mobile devices for business purposes. This program offers the convenience of using an approved non-government furnished/personally owned mobile device to access, process, transmit, or store IRS information. Therefore, those IRS employees who choose to participate in the program shall abide by the requirements specified within this policy. The IRS shall be able to ensure that agency data is protected at all places and all times. Each of the GFD and BYOD devices and the employee participant typically have a profile that is created just for them. This allows for installing and managing enterprise applications. IRS applications placed on a GFD and BYOD smart device will work on the BlackBerry (BB) server-based solution which ensures data is encrypted and cannot be copied to other applications on the mobile devices. The BB server-based solution monitors when smart devices have been tampered with and allows administrators to wipe these "jail broken" devices remotely. Please see IRM 10.8.26.3.1.1.1 (07-21-2020) for GFD sensitive information control.

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

Mailing address

Phone Numbers

E-mail Address

Date of Birth

Place of Birth

Standard Employee Identifier (SEID)

Mother's Maiden Name

Internet Protocol Address (IP Address)

Criminal History

Medical Information

Certificate or License Numbers

Vehicle Identifiers

Financial Account Numbers

Photographic Identifiers

Tax Account Information

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:

Procurement sensitive data Contract proposals, bids, etc.

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.

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

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)

PII for personnel administration is 5 USC

PII about individuals for Bank Secrecy Act compliance 31 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.

UEM Wireless application does not collect SSN information. However, data from within these applications may contain any type of PII, i.e. Name, SSN, tax account information, criminal and/or medical information etc. and we are unable to predict types of PII. Wireless users are required to encrypt all email messages containing any PII information and all commercials apps users have been informed via warning banners on the wireless devices that the use of those apps have risks. With Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) this will be captured so it does not leave the IRS unencrypted but within the email system it is possible for SSN to be part of the body of an email. 26 USC 6109 authorizes the IRS to request SSNs when necessary.

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

The BlackBerry applications only collect the employee name and SEID and does not collect SSN information. However, emails received within the BlackBerry Work application may contain any type of PII, i.e. Name, SSN etc. via Outlook and we are unable to predict types of PII in encrypted emails. Users are required to encrypt all email messages containing any PII information. 26 USC 6109 authorizes the IRS to request SSNs when necessary. Commercial apps have security banners that explains the risk of using PII when applications are outside of the containerized applications.

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

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.?

Yes

Briefly explain how the system uses the referenced technology.

These are mobile applications that enables users/participants to get IRS email or application related data on their mobile devices.

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?

Employee's name and SEID are both required to provision them on the backend BlackBerry server so that they are authenticated when accessing their IRS email account and importing their security certificates for encrypted emails. Users may receive SSNs and other PII via email as a part of their normal job function. 26 USC 6109 authorizes the IRS to request SSNs when necessary. BYOD is a self-service program and allows the user to provision their own device without assistance from IT. BYOD users are required to take a training and sign a user agreement. GFDs are provisioned when the employee signs their OL5081 after all approvals are completed. In signing the OL5081 users are agreeing to follow the IRS rules on the use of IRS IT equipment. When the GFD is sent to users, no personal accounts are able to be added to the device. The user is sent an email providing a password to complete the activation of the GFD Smartphone. The GFD Smartphone group is currently working with Advanced Services to require users to take training and sign user agreement.

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):

Users have the option to decline/opt out at any point during the process. They can also opt out of BYOD at any time after they receive approval to participate in the BYOD program.

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

We can only audit use of the GFD wireless devices and BYOD solution (e.g. BlackBerry Work app) and are not collecting audit information on the personal use of the BYOD device outside the IRS BYOD solution. All GFD and BYOD participants/users must sign a User Agreement (UA) and in doing so agree to the terms and conditions of participating in the wireless program. Below are excerpts from the BYOD UA that address (in part) due process. GFD has similar written UA displayed on its device banner before a user can activate their device. IRS IT reserves the right to disconnect my personally-owned mobile device from IRS system resources if my mobile device is used in a way that puts IRS systems or data, or the data of taxpayers or other users at an unacceptable risk of harm or disclosure. I acknowledge and consent to my personally-owned mobile device being remotely inspected and monitored using technology centrally managed by IRS IT. Devices that have not been approved for

BYOD use by IRS IT, are not in compliance with IRS security policies, or represent any unacceptable risk to the IRS network or data, will not be allowed to connect to IRS system resources. I acknowledge and understand U.S. Government systems are for authorized use only and that use of IRS systems constitutes my consent to monitoring, interception, recording, reading, copying, or capturing by authorized personnel of all activities. In agreeing to voluntarily participate in the BYOD Program, I acknowledge having no expectation of privacy regarding my use of the personally-owned mobile device approved for use in the Program. I understand and acknowledge that as with IRS-issued equipment, IRS IT can and will compile audit trails in connection with my use of my mobile device, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the IRS network, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to the IRS network may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties."

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: Administrator

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

The Administrators of the backend BlackBerry UEM servers had to submit an OL5081 to request to be added to the PRIV-DSS-MITS-EUES-TIC PRIV Role Group. The OL5081 request was approved by each of their first line managers and then finally approved by Enterprise Operations (EOPs). EOPs is the IT organization that is responsible for all servers in the IRS. The help desk support team have been granted limited access to the BlackBerry servers (BB UEM management console) by the Administrators for the sole purpose of provisioning participants. They do not have any rights to the server's operating 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?

No

Describe the system's audit trail.

Windows Server 2012 R2's native event log is used to record the following events: - Starting and stopping the BlackBerry system services and processes (tasks performed by administrators); - Device pausing and un-pausing (automated actions taken by BlackBerry in response to conditions in Exchange such as mailboxes over quota or incorrect permissions on mailboxes); - SQL Server database maintenance. These event log entries include the data elements applicable to all Windows event logs including: date/time of event, event level (information/warning/error/success/failure), source of event (system service or process), event ID number, event task category, and description, which can contain information such as mailbox name (SEID) or email address of BlackBerry user. BlackBerry's server-based system services generate additional audit logs for recording user or administrator logon to BlackBerry UEM console, queries made to the UEM console, device account adds, deletes and changes, and automated processes not initiated by individuals. Log entries may include date/time, entry type (INFO/WARNING/ERROR), transaction number, event source, description (which may contain SEID, display name, and/or email address), internal events recorded by the UEM service, activities related to the web-based components of UEM.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

There are some Use Cases but there isn't an official System Test Plan.

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: More than 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.

We audit the use of the GFD wireless devices and BYOD solution (e.g. BlackBerry Work apps) and are not collecting audit information on the personal use of the BYOD device outside the IRS BYOD solution. All GFD and BYOD participants/users must sign a User Agreement (UA) and in doing so agree to the terms and conditions of participating in the wireless program. Below are excerpts from the BYOD UA that address (in part) due process. GFD has similar written UA displayed on its device banner before a user can activate their device. "IRS IT reserves the right to disconnect my personally-owned mobile device from IRS system resources if my mobile device is used in a way that puts IRS systems or data, or the data of taxpayers or other users at an unacceptable risk of harm or disclosure. I acknowledge and consent to my personally-owned mobile device being remotely inspected and monitored using technology centrally managed by IRS IT. Devices that have not been approved for BYOD use by IRS IT, are not in compliance with IRS security policies, or represent any unacceptable risk to the IRS network or data, will not be allowed to connect to IRS system resources. I acknowledge and understand U.S. Government systems are for authorized use only and that use of IRS systems constitutes my consent to monitoring, interception, recording, reading, copying, or capturing by authorized personnel of all activities. In agreeing to voluntarily participate in the BYOD Program, I acknowledge having no expectation of privacy regarding my use of the personally owned mobile device approved for use in the Program. I understand and acknowledge that as with IRS-issued equipment, IRS IT can and will compile audit trails in connection with my use of my mobile device, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the IRS network, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to the IRS network may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties."

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