Date of Approval: July 1, 2015 PIA ID Number: **1358**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Bring Your Own Device - Good for Enterprise, BYOD

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.

Secure Mobile Device Service, BYOD PIA 280

Next, enter the **date** of the most recent PIA. 2/13/2013

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
Yes	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
Yes	Preliminary Design/Milestone 3
Yes	Detailed Design/Milestone 4A
Yes	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	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.

Good For Enterprise Technologies offers a software solution that meets FIPS 140-2 and is a Commercial Off the Shelf (COTS) product. Pairing the Good app on a smart device with the Good server-based solution ensures data are encrypted and cannot be copied to other applications on the mobile devices. Good also monitors when smart devices have been tampered with and allows administrators to wipe these "jail broken" devices remotely. The advantages of a Bring Your Own Device (BYOD) service strategy paired with Good Technologies include: (1) Meets NIST FIPS 140-2 security requirements. (2) Supports "Best Place to Work" allowing users to choose their own devices and service plans. (3) Allows MITS to reduce the support for the GFD infrastructure. (4) Reduces the cost of device from approximate $418 annually to $182. The end-game vision would be for MITS to support one BYOD mobile smart device service and remove MITS from offering Government Furnished Devices (GFD) provisioning and support services. A BYOD service model increases user satisfaction, adds value, and supports the "Best Place to Work" initiative, since users choose their own devices; carry one device that combines both business and personal services; and can load innovative applications.

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 variations of SSN s (i.e. last 4 digits, etc.)? No

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
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
Yes	Place of Birth	No	No	No
Yes	SEID	No	No	No
Yes	Mother's Maiden Name	No	No	No
Yes	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
Yes	Criminal History	No	No	No
Yes	Medical Information	No	No	No
Yes	Certificate or License Numbers	No	No	No
Yes	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No

No	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
Yes	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	Yes

6c. Does this system contain SBU information that it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

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

Selected	SBU Name	SBU Description
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
Yes	Procurement sensitive data	Contract proposals, bids, etc.
Yes	Official Use Only (OUO) or Limited Official Use (LOU)	Documents that have been marked OUO or LOU
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
Yes	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)

No	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
Yes	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 variations) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

N/A. The Good for Enterprise application only collects the employee name and SEID and does not collect SSN information. However, emails received within the Good application may contain any type of PII, (e.g.Name, SSN etc.)via Outlook and we are unable /can not predict types of PII in encrypted emails. BYOD participants are required to encrypt all email messages containing any PII information. With 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.

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

N/A. The Good for Enterprise application only collects the employee name and SEID and does not collect SSN information. However, emails received within the Good application may contain any type of PII, (e.g.Name, SSN etc.)via Outlook and we are unable /can not predict types of PII in encrypted emails. BYOD participants are required to encrypt all email messages containing any PII information.

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
34.037	IRS Audit Trail and Security Records System

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. N/A

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? 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, cloud, global position system (GPS), biometrics, RFID, etc.? Yes

14a. If **yes**, briefly explain how the system uses the referenced technology. Good for Enterprise is a mobile app that enables one to get their email.

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?
The employee's name and SEID are both required to provision them on the Good For Enterprise server so that they are authenticated when accessing their IRS email account and importing their security certificates for encrypted emails. BYOD participants 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.

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):
Potential BYOD participants have the option to decline/opt out of BYOD 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.

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

We can only audit use of the BYOD solution (e.g.Good app) and are not collecting audit information on the personal use of the BYOD device outside the IRS BYOD solution. All BYOD participants must sign a BYOD User Agreement (UA) and in doing so agree to the terms and conditions of participating in the BYOD program. Below are excerpts from the UA that address (in part) due process. 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 mobile device 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.

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	Administrator

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? The Administrators of the Good for Enterprise 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 BYOD help desk support team has been granted limited access to the Good server by the Administrators for the sole

purpose of provisioning BYOD participants. They do not have any rights to the server's operating system.

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? No

22b. If **no**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

The Secure Mobile Device Service (BYOD) is non-recordkeeping. It is a smartphone application used to ensure the security and inadvertent disclose of business communications made by IRS staff on personal mobile devices. It is not a data repository system. No records scheduling actions for BYOD are required, however User Agreements are scheduled and are to be maintained for three years after (a user's) termination of agreement (in accordance with National Archives Job No. DAA-0058-2013-0001). These disposition instructions will be published in Records Control Schedule (RCS) Document 12990 under RCS 17 for Information Technology, item 33 when next updated.

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)? No

23.1 Describe in detail the system s audit trail. Good for Enterprise uses two methods for recording audit log data. Windows Server 2008 R2's native event log is used to record the following events: - Starting and stopping the Good system services and processes (tasks performed by administrators); - Device pausing and unpausing (automated actions taken by Good 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 Good user. Good for Enterprise's server-based system services generate the following audit logs: Good Mobile Control: - audit.log – records user or administrator logon to GMC console, queries made to GMC console, device account adds, deletes and changes, and automated processes not initiated by individuals. All log entries include date/time, entry type (INFO/WARNING/ERROR), transaction number, event source, and a description, which may contain SEID, display name, and/or email address. - error.log – contains internal events recorded by the GMC service. Includes date/time, error level, transaction ID, and description. No end-user data. - Emf.log – records activities related to the web-based components of GMC. Includes date/time, entry type, transaction number, event source, and description, which may contain SEID, display name, and email address of administrators or end users. Good Mobile Messaging: The following excerpt from the Good Mobile Messaging/Good Mobile Control Administrator's Guide describes the logging captured by the Good Mobile Messaging service: Good Mobile Messaging Server Log Every Good Mobile Messaging Server maintains a log containing a separate line for every email message and event exchanged between mailbox and handheld via that server. Use the file to check account use. The log is named

servername.access and is located in the logs directory for the server installation. Each line in the server log includes the following entries, separated by tabs: • Time - Date and time of the transaction mm/dd/yyyy hh:mm:ss time zone • Msg id - The session ID of the message or event ID string • App - Service or application that sent or is receiving the message or event. For example, note, task, admin. application name • Cmd - Command used by the issuing or receiving service or application command • IP - IP address of Good Mobile Messaging Server. Allows concatenation of server log files. nn.nn.nn.nn • Mailbox - Display name of the mailbox involved in the transaction name • Direction - Transaction direction (INBOUND = towards Exchange) INBOUND | OUTBOUND • Dest conn id - For use by Customer Service nnnnnnnnnn • Num byte - Size of the transaction, read or written nnnn • Status - 0 = OK. Any other number or string indicates an error condition, but is used by Customer Service only. N Good for Enterprise Diagnostic Log Good Mobile Messaging Server maintains encrypted diagnostic logs. These logs are turned on by default. The information in the logs is for use by your authorized support representative. Good Mobile Control Server maintains encrypted diagnostic logs as well, turned on by default.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. There are some Use Cases but there isn't an official System Test Plan.

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: Not Applicable
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? No

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