Date of Approval: May 20, 2016 PIA ID Number: **1721**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Toolkit Suite With Command Centre, TSCC

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.

Toolkit Suite With Command Centre, TSCC, PIA-391, Operations & Maintenance

Next, enter the **date** of the most recent PIA. 6/19/2013

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

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.

Toolkit Suite with Command Center (TSCC) is a decision support tool with sufficient capability and data to assist the IRS with Incident Management activities (restoring or rebuilding facilities, processes, systems, or support domains from a state where existing equipment, software and technical knowledge may not be available). It is a web application that has been designated as the enterprise level repository and incident management environment for IRS information used for the development and coordination of Business Continuity, Business Resumption and Disaster Recovery Plans. TSCC also serves as a control platform for Plan deployment and Incident Management through the Command Centre Module. TSCC includes the Threat Response Center (TRC) module that is the physical threat and incident reporting system for the IRS and is owned by the Agency Wide Shared Services organization.

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.)? 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	No	No
No	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
No	Date of Birth	No	No	No
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
No	Employment (HR) Information	No	No	No
No	Tax Account Information	No	No	No

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)

No PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a

No 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.

TSCC is a plan repository and a decision support tool. It can be used by IRS executives and incident managers to assess incident/event impact and execute relevant recovery plans. During an incident or emergency event, other Systems of Record (ie TFIMS) may not be available. TSCC provides those critical data extracts in a robust system with redundancy and automated failover.

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

Data will be updated based on the data refresh cycle of the source database, but not less than monthly. Data will be verified in the Test and Development instance of TSCC sited at the Martinsburg Computing Center. TSCC receives data from other IRS systems which have their own verification process for data accuracy, timeliness, completeness, TSCC assumes that the data is accurate, timely, and complete when it is provided by other IRS systems.

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
Treasury/IRS 34.037	IRS Audit Trial and Security Records
Treasury/IRS 36.006	General Personell and Payroll Records

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. ## Redacted Information For 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
EGL	No		No	
CAU	No		No	
PDT	No		No	
PARIS	No		No	
GSS-17 ESD CADS	Yes	06/29/2015	Yes	05/14/2015
HRConnect	No	06/29/2015	No	05/14/2015
GDI Portal	No	06/29/2015	No	05/14/2015

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 agency (-ies)? No

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

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

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, cloud, 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?
This is a purely internal system and is not the official system of record. It does not make any determinations on its own. The individual's information is received from a system that provides employees with notice and rights to consent and/or amend, as needed. Notice comes through such communications as the Privacy Act notification on HR Connect and e-Performance, SETR, and

other personnel systems. Employee rights are covered through appropriate legal and NTEU contractually negotiated process for remediation.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? Other IRS systems provide data. TSCC receives monthly downloads (in the form of specified reports) from primary Systems of Record as previously specified. This data is put through an automated transform before inclusion within TSCC. This is an import only function. Other systems do not electronically access the data within TSCC.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The data is employee owned and comes as a consequence of employment. The data is received from upstream systems; any corrections would come through the data flow.

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 and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Read and Write
Developers	No	

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? Access to the data within the system is highly restricted. Users are restricted, by security role, to only that data or those pieces of the system to which they need access. Procedures and controls for TSCC are documented in the Security 1, System Security Plan (SSP), dated February, 2016. The user's profile and roles are assigned by his/her manager on IRS Form 5081, which is reviewed by the TSCC System Administrator, and established when user accounts are created. A user's position and need-to-know determines the level of access to the data. The System Administrator grants approval for system access. A user's access to the data terminates when the user no longer requires access to TSCC. Criteria, procedures, controls, and responsibilities regarding access are documented in the eBRP R4 Toolkit Admin Guide. Access to TSCC is accomplished through the I&A functions contained within enterprise implementation of Microsoft Active Directory and the specific TSCC account built within the application. This system requires all users to identify themselves and provide proof of their identities by user identification (USERIDs) and authentication (passwords). USERIDs and passwords are unique to each user. TSCC contains a number of access levels for users based upon their necessary function within the organization. Compartmentalized access must be specifically added to enable each approved user, interaction with plan data. Approved users can be assigned to any particular functional area (such as those contained within categories: Locations, Reports, Plans, etc.), and personal permissions can be set to Read Only, Read/Write, or Full Control. A users access could be as restricted as the ability to read a single document, all the way up to full control of the entire system, with any combination of features in between. TSCC stores information protected under the Privacy Act of 1974. Such information is categorized as SBU.

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.

All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6. Information ages off (is deleted from) the database at varying intervals. All records housed in the “Toolkit Suite” will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives approval to affect data disposition. Any records generated and maintained by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be destroyed using IRS General Records Schedule (GRS) 3.2, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. IRS Standard Tape Retention (IRM 2.7.6 MITS Operations, Systems Scheduling, 2.7.6.29 Tape Retention Standards) requirements stipulate that (1) Retention standards and guidelines ensure the ability to process data to completion and to permit reconstruction of data in the event of loss during processing, shipment, or disaster/business interruption. (2) The impact of extended retentions on magnetic media must be carefully considered. Media kept "on the shelf" with extended retentions beyond a reasonable period solely to protect against a remote possibility of error or disaster serves no useful purpose. It also requires additional magnetic media to be procured to meet current processing needs. Retention periods must therefore be of the minimum duration consistent with providing adequate safeguards against operational or systemic failures, disaster recovery, and with providing business interruption needs. (3) Program developers determine retentions using a number of factors and are generally found in the program COH. Sites must not deviate from the prescribed retention periods. Exceptions are noted below in the Requesting Changes to File Retentions section.

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? 6/18/2015

23.1 Describe in detail the system s audit trail. Date and Time, Standard Employee Identifier (SEID), Type of Audit Event, Subject of Audit Event, Origin of Request, Role of User and Success or Failure of Event.

J. PRIVACY TESTING

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

24c. If **no**, please explain why. TSCC is in the operation & maintenance phase. A System Test Plan is N/A

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? Yes

25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request? Yes

If **yes,** provide the date the permission was granted. 3/10/2015

25b. **If yes**, was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy? Yes

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