Date of Approval: 06/11/2025
Questionnaire Number: 2125

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Toolkit Suite with Command Centre

Acronym:

TSCC

Business Unit

IT - Cybersecurity

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

Toolkit Suite with Command Centre (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 also includes the Threat Response Centre (TRC) module that is the physical security threat reporting system for the IRS and is used by the Facilities Management & Security Services (FMSS) organization within the

Situational Awareness Management Center (SAMC). TRC is used by all IRS employees to submit physical security threat tickets to SAMC for processing, escalation, and management.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

TSCC/TRC uses SBU/PII in four ways: 1. An updated roster of all IRS employees is required to function. This personnel data is imported/updated on a weekly basis from the Corporate Authoritative Directory Service (CADS) database and was implemented in direct coordination with the CADS team. Personnel data is limited to name, Post of Duty (POD), Standard Employee Identifier (SEID), work email address, work phone, position, manager name, manager SEID, and organization/department name. 2. Physical Security Threats may be submitted by any employee to the Facilities Management & Security Services (FMSS) Situational Awareness Management Center (SAMC) via the TRC web-based ticketing interface. Tickets include the employee data and may include sensitive information such as health-related data (i.e., COVID-19 status) or details regarding specific threats against the IRS. Tickets are processed by the SAMC and may have other sensitive data added to them as an incident evolves. This data may include PII regarding perpetrators of threats such as name, address, criminal history, and/or photographic and vehicle identifiers. Perpetrators are often non-IRS individuals, i.e., Taxpayers. 3. Detailed IT System Contingency Plan (ISCP) data including instructions regarding the recovery of these systems is stored and managed within TSCC. 4. Detailed Occupant Emergency Plans (OEP) for all IRS facilities are stored within TSCC.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address
Criminal Record
Email Address
Employment Information
Medical History/Information
Name
Other
Photograph
Standard Employee Identifier (SEID)

Telephone Numbers
Vehicle Identification Number (VIN)

Please explain the other type(s) of PII that this project uses.
Other is referring to details regarding specific threats against the IRS. This is reported within our Threat Response Centre (TRC) Module

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
PII for personnel administration - 5 USC

Product Information (Questions)

1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?
No

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?
System

3 What Tier designation has been applied to your system?
3

4 Is this a new system?
No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?
Yes

4.11 What is the previous PCLIA number?
6815

4.12 What is the previous PCLIA title (system name)?
Toolkit Suite with Command Centre, TSCC

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)
Expiring PCLIA

5 Is this system considered a child system/application to another (parent) system?
No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

Execution

7 Is this a change resulting from the OneSDLC process?

No

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

Cybersecurity and Privacy Management Level Governance Board.

9 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.

211087

10 If this system discloses any PII to any third party outside the IRS, does the system have a process in place to account for such disclosures in compliance with IRC 6103(p)(3)(A) or Subsection c of the Privacy Act?

No

10.1 You have indicated that you do not have an "accounting of disclosures" process is in place; please indicate a projected completion date or explain the steps taken to develop your accounting of disclosures process. Note: The Office of Disclosure should be contacted to develop this system's accounting of disclosures process.

The system does not include or require disclosure of tax or employee information to anyone. There is not a projected completion date.

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

No

12 Does this system use cloud computing?

No

13 Does this system/application interact with the public?

No

13.1 If the system requires the user to authenticate, was a Digital Identity Risk Assessment (DIRA) conducted?

No

13.11 Please upload the approved DIRA report using the Attachments button. Select "Yes" to indicate that you have or will upload the signed DIRA form.

No

13.2 If individuals do not have the opportunity to give consent to collect their information for a particular use, why not?

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, Single Entry Time Reporting (SETR), and other personnel systems.

13.3 If the individual was not notified of the following items prior to the collection of information, why not? 1) Authority to collect the information 2) If the collection is mandatory or voluntary 3) The purpose for which their information will be used 4) Who the information will be shared with 5) The effects, if any, if they don't provide the requested information.

Notice is provided to the individual prior to collection of information. Before the individual can access the system, they are greeted with a banner that informs the individual of the items listed.

13.4 If information is collected from third-party sources instead of the individual, please explain your decision.

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, Single Entry Time Reporting (SETR), and other personnel systems. Employee rights are covered through appropriate legal and National Treasury Employees Union (NTEU) contractually negotiated process for remediation.

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

The data is employee owned and comes because of employment. The data is received from upstream systems; any corrections would come through the data flow.

15 Is this system owned and/or operated by a contractor?

Toolkit Suite with Command Centre (TSCC) is not operated by a contractor. TSCC is a COTS product that is developed by eBRP Solutions Network INC.

15.1 If a contractor owns or operates the system, does the contractor use subcontractors; or do you require multiple contractors to operate, test, and/or maintain this system?

No

15.2 What PII/SBU data does the subcontractor(s) have access to?

Toolkit Suite with Command Centre (TSCC) is not operated by a contractor. TSCC is a COTS product that is developed by eBRP Solutions Network INC. We have a support contract, but all work is performed by System Administrators and Database Administrators who are IRS employees.

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

TSCC is a COTS product. It is operated solely by IRS staff, but it is developed externally by the developer, eBRP Solutions Network, Inc. There are no users or roles that are external to the IRS. The following internal IRS user types (roles) have access to the system with the specified rights:
Employee Users: Read/Write based on principle of Least Privilege
Employee Managers: Read/Write based on principle of Least Privilege
Employee System Administrators: Read/Write based on principle of Least Privilege
Employee Developers: N/A - there are no internal developers for this system
Contractor Users: Read/Write based on principle of Least Privilege
Contractor Managers: Read/Write based on principle of Least Privilege
Contractor System Administrators: Read/Write based on principle of Least Privilege
Contractor Developers: None

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

We are collecting your personal information to facilitate access to internal IRS systems or applications and allow IRS to track use of its information technology resources as authorized by 5 U.S.C. 301. The information may consist of: Name Email Address Username UserID Password PIV Credentials SEID Number Device ID We may disclose this information in accordance with the applicable Routine Uses published in the Treasury/IRS 34.047 IRS Audit Trail and Security System and Treasury .015 General Information Technology Access Account Records System of Records Notices. Providing your personal information is voluntary and necessary to access IRS internal systems and applications. By giving us your information, you consent to its use for this purpose. If you choose not to provide your information your access may be denied. Other internal

systems that collect more than this information from you must include a unique Privacy Act statement as you access them.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

More than 100,000

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

More than 10,000

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

Not applicable

22 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). The user's profile and roles are assigned by his/her manager on IRS Business Entitlement Access Request System (BEARS), 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.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

No

24 Explain any privacy and civil liberties risks related to privacy controls.

No - TSCC is currently in the Operations and Maintenance phase of its lifecycle. Continuous Monitoring (now called Annual Security Control Assessment (ASCA)) occurs annually to ensure that controls remain in place to properly safeguard PII.

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

No

26 Describe this system's audit trail in detail. Provide supporting documents.

In the current application database, audit trailing is implemented. The audit trail is a feature of Toolkit Suite with Command Centre (TSCC). IRM 10.8.1.4.3 requires auditing processes on each table and event, including changes to employee PII. This auditing will include capturing the following: insert date and time, "user(s)"

affected by the change, the fields changed, user responsible for the changes. TSCC is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

27 Does this system use or plan to use SBU data in a non-production environment?
Yes

27.1 Please upload the Approved Email and one of the following SBU Data Use Forms, Questionnaire (F14664) or Request (F14665) or the approved Recertification (F14659). Select Yes to indicate that you will upload the Approval email and one of the SBU Data Use forms.
Yes

Interfaces

Interface Type
IRS Systems, file, or database
Agency Name
Graphic Database Interface (GDI)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Electronic File Transfer Utility (EFTU)

Interface Type
IRS Systems, file, or database
Agency Name
Corporate Authoritative Directory Service (CADS)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Electronic File Transfer Utility (EFTU)

Interface Type
IRS Systems, file, or database
Agency Name
ServiceNow
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method

Shared Drive (Shared drive has File level permissions)
\\Vp0smemwebbit01.ds.irsnet.gov\irworks1\OUTGOING

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 36.003 - General Personnel and Payroll Records

Describe the IRS use and relevance of this SORN.

All user's name, POD, SEID, work email address, work phone, position, manager name, manager SEID, and organization/department name.

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

All user activities within the system can be queried via SEID and/or name for purpose of security audit.

Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

GRS 3.2 Information Systems Security Records

What is the GRS/RCS Item Number?

050

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Electronic copy, considered by the agency to be a federal record, of the master copy of an electronic record or file and retained in case the master file or database is damaged or inadvertently erased.

What is the disposition schedule?

Temporary. Destroy immediately after the identical records have been captured in a subsequent backup file or at any time after the transfer request has been signed by the National Archives, but longer retention is authorized if required for business use.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

GRS 3.2 Information Systems Security Records

What is the GRS/RCS Item Number?

040

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Backup files maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

What is the disposition schedule?

Temporary - Destroy when superseded by a full backup, or when no longer needed for system restoration, whichever is later.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

GRS 3.2 Information Systems Security Records

What is the GRS/RCS Item Number?

041

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Backup files maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

What is the disposition schedule?

Temporary - Destroy when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

GRS 3.2 Information Systems Security Records

What is the GRS/RCS Item Number?

051

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Electronic copy, considered by the agency to be a federal record, of the master copy of an electronic record or file and retained in case the master file or database is damaged or inadvertently erased.

What is the disposition schedule?

Temporary. Destroy immediately after the identical records have been deleted or replaced by a subsequent backup file, but longer retention is authorized if required for business use.

Data Locations

What type of site is this?

SharePoint Online (SPO) Collection

What is the name of the SharePoint Online (SPO) Collection?

Information Technology Continuity Services (ITCS) Internal Team Site

What is the sensitivity of the SharePoint Online (SPO) Collection?

Personally Identifiable Information (PII) including Linkable Data

What is the URL of the item, if applicable?

https://irsgov.sharepoint.com/sites/ITEOpsITCS1yb

Please provide a brief description of the SharePoint Online (SPO) Collection.

This site houses IRS business phone numbers and emails as well as personal phone numbers and in some cases personal emails. The site also houses points of contact for the application vendors and the application service support points of contact (phone numbers, email, etc.) for the Toolkit with Command Centre (TSCC) team to maintain the TSCC application.

What are the incoming connections to this SharePoint Online (SPO) Collection?

Incoming connections to the SharePoint Online Collection are internal to the IRS. IRS personnel access the SPO via Single Sign On (SSO).

What are the outgoing connections from this SharePoint Online (SPO) Collection?

All outgoing connections to this site are IRS intranet connections.