



EFFECTIVE DATE

(06-27-2022)

PURPOSE

- (1) This transmits a revised IRM 4.7.2, Examination Returns Control System (ERCS), Security.

MATERIAL CHANGES

- (1) Due to the move of the ERCS server from Solaris to Linux logins based on the user names are no longer used. The login is now the user's Standard Employee Identifier (SEID) in lower case letters.
- (2) Due to the move to Linux access to ERCS is through Active Directory and passwords are no longer used. References to passwords have been removed throughout this IRM.
- (3) The IRS replaced the Online 5081 (OL5081) system with the Business Entitlement Access Request System (BEARS). References to OL5081 have been replaced with BEARS throughout this IRM.
- (4) Due to the move to Linux new BEARS applications for ERCS were created following the BEARS naming conventions. Application names have been updated throughout the IRM.
- (5) Content from the AIMS/ERCS website was required to be moved to the Virtual Library. ERCS content was moved to the ERCS book under the Exam Systems Knowledge Base. References to the AIMS/ERCS website have been replaced with the ERCS book throughout this IRM.
- (6) Significant changes to this IRM are reflected in the table below:

Original Reference	New Reference	Description of Change
N/A	4.7.2.1.1 (3)	"Background": Added new paragraph, per IRS security requirements, IT employees are not permitted to have access to taxpayer data.
N/A	4.7.2.1.6	Added "Defined Terms" in the internal controls section.
4.7.2.2.1 (1), 4.7.2.2.1 (2), 4.7.2.2.1 (3), 4.7.2.2.1 (4)	N/A	Under "Meeting the Prerequisites" paragraphs pertaining to background checks were removed, as all employees undergo a cursory investigation prior to an offer of employment.
4.7.2.2.4	N/A	Removed "ERCS Login Names and Passwords" as ERCS no longer requires a password, the login name is the user's SEID in lower case letters, and ERCS no longer has network printers.

Original Reference	New Reference	Description of Change
4.7.2.2.5	N/A	Removed “Changing a Login Name” as the login name is now the user’s SEID in lower case letters.
4.7.2.3.1	4.7.2.3.1	Under “ERCS Employee Records” clarified where the user can find assistance when receiving an invalid SEID message when adding a new employee record.
4.7.2.3.2.1	4.7.2.3.2.1	Under “Recommended Permissions” recommendations for SBSE and LB&I Territory Managers was added.
4.7.2.4	4.7.2.4	Under “Getting Assistance” clarified issues must be reported to the local AIMS/ERCS staff to be elevated to the HQ ERCS analysts if the issue cannot be resolved at the local level. OS GetServices tickets should only be input by the HQ ERCS analysts.

- (7) Minor editorial changes have been made throughout this IRM. Some items were reworded for clarity. Also, website addresses and IRM references were reviewed and updated, as necessary.

EFFECT ON OTHER DOCUMENTS

IRM 4.7.2 dated October 11, 2019 is superseded.

AUDIENCE

Small Business/Self Employed (SB/SE), Large Business and International (LB&I), Tax Exempt & Government Entities (TE/GE) and Headquarters (HQ) employees in Return Preparer Office (RPO), and Whistleblower Office (WO) who use ERCS.

Lori L. Roberts
 Director, Technology Solutions
 Small Business/Self-Employed

4.7.2
Security

Table of Contents

- 4.7.2.1 Program Scope
 - 4.7.2.1.1 Background
 - 4.7.2.1.2 Authority
 - 4.7.2.1.3 Responsibilities
 - 4.7.2.1.4 Program Controls
 - 4.7.2.1.5 Acronyms
 - 4.7.2.1.6 Defined Terms
 - 4.7.2.1.7 Related Resources
 - 4.7.2.2 ERCS Access
 - 4.7.2.2.1 Meeting the Prerequisites
 - 4.7.2.2.2 Choosing the BEARS Application
 - 4.7.2.2.3 Completing the BEARS Request
 - 4.7.2.3 Security Features of ERCS
 - 4.7.2.3.1 ERCS Employee Records
 - 4.7.2.3.2 Permissions
 - 4.7.2.3.2.1 Recommended Permissions
 - 4.7.2.3.3 Employee Audit Security
 - 4.7.2.3.4 Audit Trails
 - 4.7.2.3.5 Audit Trail Review
 - 4.7.2.4 Getting Assistance
- Exhibits
- 4.7.2-1 Acronyms and Definitions
 - 4.7.2-2 ERCS BEARS Applications for CCP
 - 4.7.2-3 ERCS BEARS Applications for TS
 - 4.7.2-4 ERCS BEARS Applications for Specialty and WEIC
 - 4.7.2-5 ERCS BEARS Applications for SBSE
 - 4.7.2-6 ERCS BEARS Applications for LB&I

4.7.2.1
(06-27-2022)
Program Scope

- (1) This IRM section discusses ERCS security and procedures for controlling and maintaining ERCS access.
- (2) **Purpose:** To provide guidance needed to complete the correct Business Entitlement Access Request System (BEARS) ERCS application and provide recommendation for approval and granting of permissions based upon the user's official duties.
- (3) **Audience:** ERCS is used by employees in SB/SE, LB&I, TE/GE, and Headquarters (HQ) employees in the Return Preparer Office (RPO), and Whistleblower Office (WO) who monitor inventory, enter examination time, add new records or update existing records on ERCS. Employees include analysts, managers, technical employees, administrative support personnel and shared administrative support personnel.
- (4) **Policy Owner:** The SB/SE Deputy Director, Examination, who is under the SB/SE Director, Examination.
- (5) **Program Owner:** SB/SE Director, Technology Solutions.
- (6) **Primary Stakeholders:** LB&I.

4.7.2.1.1
(06-27-2022)
Background

- (1) All ERCS users, their managers, and ERCS support personnel (including system administrators, database administrators and ERCS developers) should be familiar with this IRM to ensure they are aware of the system security features and the requirements for ERCS access.
- (2) Users must be aware of the potential for Unauthorized Access of Taxpayer Accounts (UNAX) violations from the use of ERCS. Data from ERCS should be accessed only for IRS business purposes. Users should promptly retrieve ERCS reports from printers or fax machines in order to prevent unintentional disclosure. Audit trails are created and subject to review for all user accesses of taxpayer data. For more information about UNAX, see IRM 10.5.5, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance, and Requirements..
- (3) Per IRS security requirements, IT employees are not permitted to have access to taxpayer data. No IT employee should be approved for ERCS access and any user transferred or detailed to an IT position must submit a Remove Access request to have all permission records removed.

4.7.2.1.2
(06-27-2022)
Authority

- (1) IRM 10.8.1, Policy and Guidance, establishes the security program and the policy framework for the IRS.

4.7.2.1.3
(06-27-2022)
Responsibilities

- (1) Ensuring the security of ERCS is the responsibility of every user and support personnel including the AIMS/ERCS staff, the ERCS system and database administrators, and the ERCS developers.
- (2) **ERCS User Responsibilities:** All users are responsible for ensuring the security of the ERCS system. This includes but is not limited to the following:
 - Removing Smart Cards before leaving work stations
 - Promptly picking up ERCS prints from printers in common areas
 - Updating and approving work timely and accurately

4.7 Examination Returns Control System (ERCS)

- Protecting taxpayer data from unauthorized access
 - Reporting security incidences to the proper authorities timely
- (3) **AIMS/ERCS (A/E) Staff Responsibilities:** In addition to user responsibilities, the A/E staff security responsibilities include but are not limited to the following:
- Ensuring users have met the prerequisites before approving BEARS requests for ERCS access
 - Granting user access based on and limited to the user’s official duties and deleting permission records when no longer needed
 - Training and/or providing job aids to new users regarding security requirements
 - Ensuring the continued integrity of the ERCS database, which includes reviewing and correcting data issues and participating in operational reviews based on IRM requirements and local procedures
- (4) **System Administrator (SA) Responsibilities:** The ERCS system administrator responsibilities include but are not limited to:
- Ensuring all security features are installed and operating properly on the ERCS server.
 - Working OS GetServices tickets to resolve ERCS system related user issues.
- (5) **Database Administrator (DBA) Responsibilities:** The database administrator responsibilities include but are not limited to:
- Ensuring all Oracle security features are installed and operating properly.
 - Working OS GetServices tickets to resolve ERCS database related issues.

4.7.2.1.4
(10-11-2019)

Program Controls

- (1) ERCS creates audit trails for selected changes to returns, employee records, and permission records. A special audit trail is also created when users enter a taxpayer identification number (TIN) or a taxpayer name on ERCS.
- (2) There are security checks within ERCS to ensure unauthorized users do not access programs and authorized users are kept within the boundaries of their permissions. These checks are performed automatically and silently each time a user attempts to access ERCS. The user has no ability to prevent the checks.

4.7.2.1.5
(06-27-2022)

Acronyms

- (1) See Exhibit 4.7.2-1, Acronyms and Definitions, for acronyms used in the IRM.

4.7.2.1.6
(06-27-2022)

Defined Terms

- (1) The following are defined terms for this IRM:

Term	Definition
Login	The user’s SEID with lower case letters.

Term	Definition
Detail	<ul style="list-style-type: none"> • Temporary reassignments to another group or function for less than one year, and is expected to return to the original group. • Acting as a group manager (including the employee's own group) which involves a change in grade, position, and/or group assignment. • Details out of the Area expected to last one year or less.
Acting	<ul style="list-style-type: none"> • Technical employee retains work assignments and inventory, while temporarily acting as manager of their own group. • Manager is on leave or otherwise out of the office. • There is no change of grade or group assignment.
Transfer	<ul style="list-style-type: none"> • Permanent reassignments to another group or function. • Rotational assignments from one to five years in length. • Details out of the Area expected to last longer than one year.

4.7.2.1.7
(06-27-2022)

Related Resources

- (1) The following resource documents contain information regarding IRS security requirements and ERCS programs related to creating and reading ERCS audit trails:
 - IRM 10.8.1, Policy and Guidance
 - *Security* chapter of the ERCS Technical Reference Manual (TRM)
 - Read Audit Trails section of the *Utility Miscellaneous Programs* chapter of the ERCS TRM
- (2) The *ERCS book* in the Virtual Library contains helpful information to resolve problems and answer questions. The following types of information is available:
 - *Manual and Handbooks* - this section contains the ERCS user handbooks and the ERCS TRM. The manuals describe the menu options, screens, reports and other relevant information.
 - *Troubleshooting* - this section has information on current issues such as installing the ERCS session file and the Invalid SEID error message.
 - *Contacts* - this section contains contact information for AIMS/ERCS Staff, Area and Campus Programs, Employee Group Codes, LB&I Contacts, and other helpful contact information.
- (3) For security issues concerning record of tax enforcement results (ROTTER) information, see the *Section 1204 Website*. IRM 1.5, Managing Statistics in a Balanced Measurement System, provides further guidelines for the appropriate use of statistics by managers and employees.

4.7 Examination Returns Control System (ERCS)

4.7.2.2 (06-27-2022) ERCS Access

- (1) Managers must ensure that employees are only given ERCS access if their job requires it. Managers must also ensure access is removed timely when the employee's job no longer requires ERCS access or the employee is transferring from their group. Permission must be restricted so the employee only has what is necessary in order to perform official duties.
- (2) This section discusses the requirements for obtaining and maintaining access to ERCS programs and data. The following topics are included:
 - Meeting the prerequisites
 - Choosing the BEARS Application
 - Completing the BEARS Request

4.7.2.2.1 (06-27-2022) Meeting the Prerequisites

- (1) Employees must have reported to the group before access to ERCS is requested.
- (2) Employees must have completed a UNAX Briefing and UNAX Certification prior to being given access to ERCS data. The employee's manager is responsible for ensuring this has been completed prior to approving the BEARS Add Access request.
- (3) Employees hired into a position requiring ERCS access are granted access on the approval of their managers and the A/E staff. These positions include:
 - Exam group managers in SB/SE and their administrative support staff
 - Team managers in LB&I and their administrative support staff
 - Territory managers (TM)s and SB/SE Area administrative support staff
 - Territory managers, Directors of Field Operations (DFO)s, and LB&I Practice Area administrative support staff
 - Planning and Special Programs (PSP) chiefs, section chiefs, program coordinators, technical employees and their administrative support staff
 - Technical Services (TS) managers, selected technical employees and their administrative support staff
 - Joint Committee Review (JCR) managers and their administrative support staff
 - National Quality Review System (NQRS) managers and their administrative support staff
 - Quality Review & Analysis (QRA) managers and their administrative support staff
 - Centralized Case Processing (CCP) managers and selected members of their staff
 - Return Preparer Office (RPO) administrative support staff
 - A/E managers, analysts, assistants and their administrative support staff
 - HQ ERCS analysts

Note: An employee detailed into a position above or acting for an employee in a position above, may also be granted access for the duration of the detail or acting assignment.

- (4) An employee may be granted access on the approval of their manager and an HQ ERCS analyst if there is justification that access is needed in order to perform the user's official duties. These employees include the following:
 - SB/SE and LB&I HQ analysts
 - RPO analysts

- NRP analysts
- WO employees

(5) Shared administrative associates from TE/GE and SB/SE Collections supporting SB/SE and LB&I groups are required to meet the same prerequisites.

4.7.2.2.2
(06-27-2022)
**Choosing the BEARS
Application**

(1) To obtain access to ERCS, employees must complete a BEARS request. Employees may need to submit more than one request for ERCS access if permission is needed in more than one area or in both LB&I and SB/SE. If the employee requires more than one BEARS request for ERCS, the first application requested must be within the user's support area and Business Operating Division (BOD). The user should wait until they have accessed ERCS for the first time before submitting additional requests to other areas. There is an exception for HQ analysts, NRP analysts, and WO employees. Refer to IRM 4.7.2.2.2 (5) for BEARS procedures for these employees.

Note: When an LB&I user needs access to multiple groups within LB&I, regardless of PBC, only one BEARS request is needed. It should be for the area that supports the user's home group.

(2) ERCS users are supported by the A/E staff located in the user's local area or CCP campus, with the exception of employees in Fraud/Bank Secrecy Act (BSA), Withholding Exchange and International Individual Compliance (WEIIC), and WO employees. Fraud/BSA, WEIIC, and RPO users have their own A/E support staff. WO employees are supported by Area 206, Western. Refer to the *AIMS-ERCS Staff Listings* for support contact information.

(3) It is important to select the correct BEARS ERCS application because each one is routed to the local A/E staff for approval, creation of the user's ERCS employee record, work schedule profile and inputting permission records. The ERCS BEARS Application tables, Exhibit 4.7.2-2 through Exhibit 4.7.2-6, include all ERCS applications for requesting access. Except for HQ analysts, NRP analysts, and WO employees, the exhibit tables should be used to determine a user's **initial** BEARS application selection. For the excepted employees refer to IRM 4.7.2.2.2 (5).

(4) On rare occasions if access is needed to update records for an additional area or BOD, subsequent BEARS requests must be completed. Write permission across areas requires justification in the Special Instructions box on the request.

(5) HQ analysts, NRP analysts, and WO employees must have an approved BEARS request for PROD ANALYST ERCS HQ ANALYST prior to requesting any other ERCS BEARS application. This ERCS application is routed to the HQ ERCS analysts for approval. An HQ ERCS analyst will contact the employee or employee's manager to determine what level of access and permission records are needed, and then will inform the employee which subsequent BEARS ERCS application to submit. The HQ ERCS analyst will alert the A/E managers in the areas impacted to let them know that ERCS access has been granted.

(6) Information for BEARS applications for Statistical Sampling Inventory Validation Listing (SSIVL), Tableau and A/E staff are discussed in IRM 4.7.10, AIMS/

4.7 Examination Returns Control System (ERCS)

ERCS Staff. See *Headquarters Contacts for AIMS, ERCS, SETTS, SSVL, and Tableau* for contact information for the HQ analysts who support these programs.

4.7.2.2.3
(06-27-2022)

Completing the BEARS Request

- (1) BEARS requests for new users must contain sufficient information for the A/E analyst to add the employee's permission records on ERCS as this document serves as the official record of the user's approved level of access. The following information must be included in the Special Instructions box, either by the employee, the employee's manager, or the A/E analyst:

- a. User's login, this will be the employee's SEID with lower case letters.
- b. AIMS Assignee Code (AAC) or AACs - The Primary Business Code (PBC), Secondary Business Code (SBC), and Employee Group Code (EGC) combination the user needs permission for in order to run reports, update records, apply time, etc. These three codes make up the 12 digit AAC.
- c. Permission type - The permission types consist of read, write, first level approval, and second level approval. With read permission users can run reports and see returns in their group. Write permission gives the user the ability to generate forms, update returns, and add or update employee records in the group. First level approval permission gives managers and acting managers the ability to approve updates made by other users in the group. In general, administrative support employees are given read and write permission, managers are given read and first level approval permission and TMs are given read and second level approval permission.

Note: Acting managers with inventory will not routinely be given write permission during an acting assignment and must not be given permanent write permission. Users requesting temporary write permission should include the requested permission in the Special Instructions box and the reason it's needed, when completing (or modifying) their BEARS request so it is included when the manager approves the form.

Note: Managers may be given write permission, temporary is preferable, with TM approval. The manager must include the requested permission in the Special Instructions box and the reason write permission is needed, when completing (or modifying) their BEARS request so it is included when the TM approves the form. The BEARS request must be approved by the TM and not by proxy.

Note: Territory managers must approve requisitions, statute updates, and transfers or closures to a return generating the command code AMSOC if made by a manager in their territory. Since an acting manager cannot approve work for returns in their own inventory, the TM may need to approve updates made to the acting manager's inventory. Therefore, if a TM approves write permissions for a manager or acting manager, they must be an active ERCS user with second level approval.

- d. User Type - (Group, PSP, Review (Technical Services), Sample Review, CCP, Territory, DFO, Area, Admin, Limited). The user type determines the menu options available to the user.

- e. Length of Access - The user should state if permanent access is needed. If the user only needs temporary access, they should include the start and ending dates of the assignment.

Note: An active BEARS request gives the user access to the ERCS server. Permission records give the user access to run ERCS programs.

Example: A user acting for the manager on an ongoing basis may need permanent access to the server, but temporary permission to approve work during each acting assignment.

Example: A user acting for the manager for a specific period of time would only need temporary access to the server and to ERCS. They would notate start and end dates in the Special Instructions box on the BEARS request.

- f. Justification - The business reason the employee needs access must be included in the Special Instructions box. If permission is needed outside the user's group or function, a justification must be input. Any other special instructions should be included such as detail assignment or acting assignment.

Note: Except for Limited Access users, examiners access to ERCS should be restricted to acting assignments.

4.7.2.3
(10-11-2019)
**Security Features of
ERCS**

- (1) In addition to numerous program validation and consistency checks to ensure data is valid, ERCS security is assured by:

- Limited system and data access by users to ensure information is provided on a need-to-know basis.
- Audit trail generation and review of users' activities.
- Electronic managerial approval of certain actions.

- (2) The following topics are included in this section:

- ERCS Employee Records
- Permissions
- Employee Audit Security
- Audit Trails
- Audit Trail Review

4.7.2.3.1
(06-27-2022)
**ERCS Employee
Records**

- (1) ERCS interfaces with the Corporate Authoritative Directory Service (CADS) to download employee information, including the employee's SEID, into the ERCS database. Only data for SB/SE, LB&I, WO, and RPO employees is downloaded. When an employee record is added to ERCS, the user enters the employee's SEID. It is validated against the downloaded employee data from CADS (Discovery Directory). If a user is unable to add a new employee to ERCS because the employee's SEID is invalid, the user should refer to the instructions on the *Invalid SEID Error Message* page under Troubleshooting in the ERCS book to resolve the issue.

- (2) Employee records are added by a user with write permission for the AAC the employee will be assigned to. This includes administrative support staff or the local A/E staff.

4.7 Examination Returns Control System (ERCS)

- (3) The information on the ERCS employee record should be entered accurately and completely. Any changes to the record should be updated as soon as they are known. ERCS employee record data is used to:
 - Verify a user is authorized to access ERCS.
 - Determine if an employee is required to charge technical time.
 - Validate the employee's AAC during inventory assignment.
 - Determine if the employee should have access to the Managerial Approval menu option.
 - Determine if an employee's actions require managerial approval.
 - Protect an employee's tax return from unauthorized access.
 - Determine who should receive employee audit security alerts.
 - Determine if the employee's tax return can be audited in the area.
 - Create ERCS audit trails.
 - Create the SETTS file.
- (4) Employee records should be updated when an employee's name changes. If an employee has been issued a pseudonym for security reasons, the pseudonym should be entered on the ERCS employee record followed by a space and the literal **XX**. This will alert the A/E staff that the name on the employee record is not the employee's real name.
- (5) ERCS employee records should be inactivated when the employee leaves the IRS or transfers within the IRS to a non-ERCS position. If the employee's time is entered on ERCS, the end date on the employee record must be set to the last day the employee is required to enter time. Otherwise, the last day the employee worked should be entered for the employee's end date. The login name should not be removed from the ERCS employee record when an employee record is inactivated. It is a link to the ERCS audit trails.
- (6) A user's login must be entered in the Login field of the employee record or the user will not be able to access ERCS.

4.7.2.3.2 (06-27-2022) Permissions

- (1) Permission records determine what menu options are available to a user within the ERCS Main Menu. They also give users the ability to run reports, update employee records and returns, input time, and approve work.
- (2) Permission records are to be added when a BEARS request is processed or the user will not be able to access ERCS.
- (3) The permission types are read, write, first level approval, and second level approval. Managerial approval can be restricted so the user can only approve updates by return. Permission records are based on AACs. For example, a group manager may be given read and first level approval permission for the group's AAC. A CCP user in Memphis may be given read and write permission for returns in Memphis CCP.
- (4) ERCS programs use the employee's permission records with the ERCS national status code files to restrict access based on the status code on the return. For example, a group user may only update returns in a group status. CCP users may only update returns in a CCP status. See Document 6036, Examination Division Reporting System Codes Booklet, for a list of status codes used by examination.
- (5) Permission records are added by the A/E staff. Managers with permanent first level approval permission can delegate temporary first level approval permis-

sion for their group to an acting manager as long as the employee has an active ERCS login. Approval permission should only be granted for the length of the acting assignment. Managers with permanent write permission may delegate temporary write permission for their group to a shared administrative support employee in another group if assistance is needed.

- (6) For permanent permission changes within the same area and temporary changes lasting over 30 days, the user is required to submit a Modify Access request via BEARS.
- (7) Permission can be permanent or temporary. Temporary permission is granted for up to 180 days, if needed for a longer period of time, permanent permission should be granted. The user will request removal of the permission records via a Remove Access BEARS request when no longer needed.
- (8) A temporary, emergency permission change within the same area may be granted by the user’s local A/E analyst. The request should be made by management via e-mail. For emergency permission not covered in these instructions, contact an HQ ERCS analyst.
- (9) If an employee acts for their manager, first level approval permission will be granted with a beginning date and an ending date covering the acting assignment. If the acting assignment ends early, and permission was delegated by the group manager, the manager will update the permission records to the correct end date, but the ERCS employee record will remain active.
- (10) When an employee record is inactivated, the ERCS program updates the employee’s permission records to end on the employee’s inactivation date.
- (11) If a user no longer needs ERCS access due to a change in position or duties, a Remove Access BEARS request must be input.
- (12) If a user is suspended from active duty the manager must input a Remove Access BEARS request for the user’s ERCS access if one isn’t systemically generated.
- (13) Access to Menu Options 11 through 19 on the ERCS Login Menu are granted via special BEARS applications. These BEARS requests go through the HQ ERCS analysts or the HQ SSIVL analysts for approval and to add the special permissions enabling the user to access the menu options. These options are described below:

Menu Option Number	Menu Option	Required Position	BEARS Application	Description
11	AIMS/ERCS Analyst Menu	A/E staff	PROD ANALYST AIMS-ERCS STAFF	This menu contains options to aid in the support of ERCS end-users.
12	SSIVL	Administrative support staff from SB/SE, LB&I, TE/GE, and W&I	PROD USER SSIVL-###	This menu contains programs associated with SSIVL including extracting data

4.7 Examination Returns Control System (ERCS)

Menu Option Number	Menu Option	Required Position	BEARS Application	Description
12	SSIVL	SSIVL Coordinators from SB/SE, LB&I, TE/GE, and W&I	PROD COORD SSIVL	This menu contains programs associated with SSIVL and maintaining the SSIVL AAC list.
13	SSIVL for CCP	Analysts and administrative support staff in CCP	PROD USER SSIVL-CCP ###	This menu contains programs associated with SSIVL including extracting data and running reports.
14	Check Mail	Security officers, PSP chiefs, A/E staff	PROD ANALYST AIMS-ERCS STAFF	This option allows users to read ERCS system e-mail.
15	AIMS Download	A/E staff	PROD ANALYST AIMS-ERCS STAFF	This menu contains the ERCS to AIMS Uploading Programs.
16	National Codes	HQ ERCS analysts, HQ SETTS analyst	PROD ANALYST AIMS-ERCS STAFF	This menu allows users to validate new codes and update national files.
17	SETTS	A/E staff	PROD ANALYST AIMS-ERCS STAFF	This menu contains the Summary Examination Time Transmission System (SETTS) programs.
18	User Administration	HQ ERCS analysts	PROD ANALYST AIMS-ERCS STAFF	This menu contains options for granting access to menu options included in this table.
18	User Administration	SSIVL analysts	PROD ANALYST AIMS-ERCS STAFF	This menu contains options for granting access to SSIVL.
19	Security	Security officers, A/E managers and analysts, and Unit Security Representatives (USR)	PROD ANALYST AIMS-ERCS STAFF	This menu contains options for reading ERCS audit trails.

4.7.2.3.2.1
(06-27-2022)

**Recommended
Permissions**

- (1) ERCS permissions are granted to users based on user type and permission type. The ten user types include:

User Type	Users
PSP	PSP section chiefs, analysts, program coordinators, technical employees and administrative support staff
Group	SB/SE and LB&I field group and tax compliance group managers, team managers, technical employees and administrative support staff, RPO administrative support staff
Territory	Territory managers and administrative support staff
DFO	Directors of field operations and administrative support staff
Area	Administrative support staff of SB/SE area directors and LB&I practice area directors. HQ analysts who need multiple Area read only access.
Review	TS and JCR managers, analysts, technical employees, and administrative support staff
Sample Review	NQRS and QRS managers and administrative support staff
CCP	CCP managers, analysts, technical employees, and administrative support staff
Admin	A/E managers, analysts and assistants. Admin users have permission to run ERCS as any user type in order to provide support for end-users.
Limited	Technical employees within an examination group, PSP, review or sample review who only have permission to input time and print their own inventory and time reports.

Note: For information about the menu options available to each user type, see the *Main Menu* chapter of the ERCS TRM.

- (2) Permanent read permission is granted to all ERCS users. Write and approval permission is granted based on the user’s need to accomplish assigned duties.
- (3) Group administrative support staff need read and write permission as a Group user for the AAC to which they are assigned and for any other AAC in which they must assist in updating returns, running reports and inputting time. LB&I administrative support staff may also be granted AMSOC Disposal Code 30 permission in order to transfer cases to other LB&I groups in a different Practice Area.
- (4) Group managers and LB&I team managers need read and first level approval permission as a Group user for the AAC to which they are assigned and for any other AAC in which the manager must assist in approving updates to returns. A group or an LB&I team manager may also be given write permission, temporary is preferable, if the territory manager is in agreement, approves the BEARS request and is an active ERCS user with Territory second level approval permission.

4.7 Examination Returns Control System (ERCS)

- (5) SB/SE and LB&I TMs need read and second level approval permission as a Territory user for the AAC to which they are assigned. They may also have first level approval for the groups in their territory in order to approve items in a manager's absence.
- (6) PSP administrative support staff need read and write permission as a PSP user for the AAC to which they are assigned and for any other AAC in which the employees must assist in updating returns, running reports and inputting time. Depending on their duties the employee may be given permission for all PSP in the area. Users responsible for transfers out-of-area should be granted AMSOC Disposal Code 30 permission, and those responsible for short closures may also be granted permission for AMSOC Disposal Codes 20, 21, 31 and 35.
- (7) In SB/SE PSP section chiefs and/or the program coordinators (depending on local procedures) need read and first level approval permission as a PSP user for the AACs in their control. The PSP program coordinators should consult with their section chief before requesting write permission since some updates input by the program coordinator require second level approval. In LB&I, PSP analysts need read and first level approval permission as a PSP user for the AACs in their control.
- (8) PSP territory managers and/or the PSP section chiefs (depending on local procedures) need read and second level approval permission for PSP in the area.
- (9) Non-managers in CCP may be given read and write permission for CCP AACs as needed to perform their duties. Users checking in and assigning inventory need write permission for the CCP campus in order to update unassigned returns.
- (10) CCP managers may be given read, write, and first level approval permission as a CCP user for their AAC.
- (11) Department managers in CCP need read permission for the CCP campus, and may be given second level approval permission, as needed.
- (12) TS administrative support staff may be given read and write permission for their review AACs. Users checking in and assigning inventory need read and write permission in order to update unassigned returns. TEs in TS may be given read and write permission for their review AACs, if needed, in order to perform their official duties.
- (13) TS managers may be given read and first level approval permission as a Review user for their AACs.
- (14) Territory managers in TS may be given Review read, first level and second level approval permission, as needed.
- (15) Sample review managers and administrative support staff need read and write for their sample review AACs.
- (16) A/E managers need Admin read permission for their area and for Areas and Practice Areas they support in Specialty and LB&I. They also need PSP read and first level approval permission for their group AAC to approve short closures.

- (17) A/E analysts and assistants need Admin read and write permission for their Area and for Areas and Practice Areas they support in Specialty and LB&I. In an emergency, temporary first or second level approval permission may be granted to an A/E analyst to approve a specific request. It's recommended that approval permission be deleted once the request is completed. A/E staff responsible for processing short closures and resubmitting short closures will be granted permission for AMSOC Disposal Codes 28, 29, 30, 33, 36, 37, 38, 39, 40, and 41. A/E analysts responsible for processing BEARS requests for ERCS access need Admin read and write permission for PBCs 320, 321, and 323-328 as permission is granted by the supporting Area for all LB&I PBCs.
- (18) HQ SB/SE and LB&I analysts may be granted Area read permission for multiple areas if access is required to perform their official duties. See also IRM 4.7.2.2.1 (4) for additional information.
- (19) HQ ERCS analysts may be granted Admin read and write permission, as needed, in order to perform their official duties.

Note: It's recommended that permission records be reviewed by the A/E staff monthly to ensure permission records are deleted when no longer needed and to verify correct permission has been granted. A permission report can be run through ERCS Tableau for review.

4.7.2.3.3
(06-27-2022)
Employee Audit Security

- (1) An employee audit occurs when the tax return of an IRS employee is examined. ERCS provides special security features for employee returns under audit. When any of the following events occur an audit trail is created and an ERCS system email alert is generated:
 - A user enters their own Social Security Number (SSN) or the SSN of a spouse (if a joint return was filed)
 - The source code on a return is changed to or from Source Code 46, "Employee Return"
 - The "Employee Audit" indicator is turned on or off on a return
 - An unauthorized user attempts to access an employee's return
 - A user attempts to add an employee return to ERCS for an employee who should not be audited in the same area
 - A employee's return is on AIMS and during AIMS to ERCS processing, the program attempts to add the return to ERCS in an area where the employee should not be audited
 - The addition of a high profile employee return to ERCS (such as the Security Officer)
- (2) If there is a Security Officer with ERCS access for the area, the employee audit e-mail is sent to the Security Officer. Otherwise, the ERCS system email is sent to the PSP TM. See IRM 4.7.5, Planning and Special Programs (PSP), for more information about the employee audit email.

Note: ERCS system email is sent and received on the ERCS server.

- (3) Not all employee audit alerts are an indication the user is doing something inappropriate. For example, alerts may be generated when a user accesses an employee's return by taxpayer identification number (TIN), and the program finds one tax period assigned to the user's group and one tax period controlled in another group or function. An alert will be generated for the tax period that is not in the user's group. Some alerts are an indication of inappropriate access,

4.7 Examination Returns Control System (ERCS)

for example, when a user enters their own SSN. See *Employee Audits* under Codes and Procedures in the ERCS book for more information.

- Note:** When an employee performs a search using the taxpayer's name and the name or name control entered matches any IRS employee, audit trails are created for each matched employee. Entering as much of the taxpayer's name as possible reduces the risk of matching an employee.
- (4) Employee returns are not included on ERCS reports and screens if the user is not authorized to see the data. In general, this means the user must have permission to the AAC of a return before the return information may be viewed, regardless of the status code. Users are not notified when an employee audit alert is generated for their access.
 - (5) For more information about employee audit security features refer to the *Security* chapter of the ERCS TRM.
- (1) An ERCS audit trail is a record of an event initiated by a user or program on the ERCS server. The event can be anything from execution of a program to accessing or changing data. Audit trails can be used to research when changes were made to data, and to determine who input or approved the changes. Audit trails can also detect potential unauthorized access or suspicious activities.
 - (2) ERCS captures audit trail information for the following events:
 - Addition or deletion of taxpayer records
 - Modification and managerial approval for selected updates to return information
 - Research of taxpayer records
 - Addition of employee records
 - Modification of selected employee information
 - Addition, deletion or modification of ERCS permissions
 - User access to the ERCS Main Menu
 - Selected events regarding employee returns under audit
 - (3) The event information captured in an ERCS audit trail includes, but is not limited to the following:
 - Time and date of the event
 - User identification
 - Approver's identification, if the action required approval
 - Type of activity (add, update, research, etc.)
 - Data that was accessed or changed
 - Program that was executed
 - (4) Audit trail information may be accessed from special ERCS menus by A/E analysts, HQ ERCS analysts, and designated system security officers. Managers should consult their local A/E staff for assistance if information from an ERCS audit trail is needed. For more information about ERCS audit trails refer to the "Read Audit Trails" section of the *Utility Miscellaneous Programs* chapter of the ERCS TRM. For information about the responsibilities of the A/E staff regarding the ERCS audit trails, see IRM 4.7.10, AIMS/ERCS Staff.

4.7.2.3.4 (06-27-2022) Audit Trails

4.7.2.3.5
(06-27-2022)
Audit Trail Review

- (1) All modernized IRS systems containing taxpayer data, like ERCS, are required to send their system and program audit trails to the Security Audit and Analysis System (SAAS). Audit trail repositories like SAAS aid the IRS and TIGTA in detecting potential unauthorized accesses to IRS systems and data.
- (2) Security specialists from Cybersecurity are responsible for performing the review of audit trails sent to SAAS. Reports from SAAS are also sent to the HQ ERCS analysts for review and verification that accesses are business related.
- (3) Refer to IRM 10.8.2, IT Security Roles and Responsibilities, for more information including actions to take for suspected security incidents.

4.7.2.4
(06-27-2022)
Getting Assistance

- (1) Users experiencing ERCS program problems or questions are to seek assistance from their local A/E staff. If the local staff cannot resolve the user's issue, they will elevate to the HQ ERCS analysts. If the HQ ERCS analysts cannot resolve the issue it will be elevated to the ERCS developers. The ERCS developers make the determination if an OS GetServices ticket needs to be input and the HQ ERCS analysts input the ticket. Tickets should not be input by the A/E staff or end-users.
- (2) For information on current issues impacting ERCS refer to the *Troubleshooting* section of the ERCS book. For information on current changes or updates impacting ERCS refer to the *What's New* section of the ERCS book.
- (3) For information on running the ERCS programs or on error messages received running ERCS, refer to the ERCS User Handbooks in the *Manual and Handbooks* section of the ERCS book.

This Page Intentionally Left Blank

Exhibit 4.7.2-1 (06-27-2022)
Acronyms and Definitions

Acronym	Definition
AAC	AIMS Assignee Code
A/E	AIMS/ERCS
AIMS	Audit Information Management System
BEARS	Business Entitlement Access Request System
BOD	Business Operating Division
BSA	Bank Secrecy Act
CADS	Corporate Authoritative Directory Service
CCP	Centralized Case Processing
DBA	Database Administrator
DFO	Directors of Field Operations
EGC	Employee Group Code
ERCS	Examination Returns Control System
HQ	Headquarters
IT	Information Technology
JCR	Joint Committee Review
LB&I	Large Business and International
NQRS	National Quality Review System
NRP	National Research Program
PBC	Primary Business Code
PSP	Planning and Special Programs
QRA	Quality Review & Analysis
ROTER	Record of Tax Enforcement Results
RPO	Return Preparer Office
SA	System Administrator
SAAS	Security Audit and Analysis System
SBC	Secondary Business Code
SB/SE	Small Business/Self Employed
SEID	Standard Employee Identifier
SETTS	Summary Examination Time Transmission System
SSIVL	Statistical Sampling Inventory Validation Listing

Exhibit 4.7.2-1 (Cont. 1) (06-27-2022)**Acronyms and Definitions**

Acronym	Definition
SSN	Social Security Number
TE	Tax Examiner
TE/GE	Tax Exempt and Government Employees
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number
TM	Territory Manager
TRM	Technical Reference Manual
TS	Technical Services
UNAX	Unauthorized Access of Taxpayer Accounts
WEIIC	Withholding Exchange & International Individual Compliance
WO	Whistleblower Office

Exhibit 4.7.2-2 (06-27-2022)
ERCS BEARS Applications for CCP

BEARS ERCS application	Location of User	BOD of User	Access needed for returns in
PROD USER LBI OGDEN CCP	Ogden Campus	SB/SE - CCP	CCP in Ogden
PROD USER SBSE CINCY CCP	Cincinnati Campus	SB/SE - CCP	CCP in Cincinnati
PROD USER SBSE MEMPHIS CCP	Memphis Campus	SB/SE - CCP	CCP in Memphis

Exhibit 4.7.2-3 (06-27-2022)**ERCS BEARS Applications for TS**

BEARS ERCS application	Location of User	BOD of User	Access needed for returns in
PROD USER SBSE AREA 202-CENTRAL	TS East	SB/SE - TS	Area 202
PROD USER SBSE AREA 203-SOUTH ATLANTIC	TS Legacy	SB/SE - TS	Area 203
PROD USER SBSE AREA 204-MIDWEST	TS Midstates	SB/SE - TS	Area 204
PROD USER SBSE AREA 206-WESTERN	TS West	SB/SE - TS	Area 206

Exhibit 4.7.2-4 (06-27-2022)

ERCS BEARS Applications for Specialty and WEIC

BEARS ERCS application	Location of User	BOD of User	Access needed for returns in
PROD USER SBSE AREA 212-EMPLOYMENT	Any Location	SB/SE - Employment Tax	Area 212
PROD USER SBSE AREA 213-ESTATE GIFT	Any Location	SB/SE - Estate & Gift	Area 213
PROD USER SBSE AREA 214-EXCISE	Any Location	SB/SE - Excise	Area 214
PROD USER SBSE AREA 217-BSA FRAUD	Any Location	SB/SE - Fraud/BSA	Area 217 (Fraud or BSA)
PROD USER SBSE AREA 218-RPO	Any Location	RPO	Area 218 (RPO)
PROD USER LBI AREA 330-WEIC	Any Location (including Puerto Rico)	LB&I	Area 330 (WEIC)

Exhibit 4.7.2-5 (06-27-2022)

ERCS BEARS Applications for SBSE

BEARS ERCS application	Location of User	BOD of User	Access needed for returns in
PROD USER SBSE AREA 201-NORTH ATLANTIC	Connecticut, Maine, Massachusetts, New Hampshire, New Jersey, New York, Rhode Island, Vermont	<ul style="list-style-type: none"> • SB/SE, excluding TS • SB/SE Collec- tions, LB&I and TE/GE shared administrative associates 	Area 201
PROD USER SBSE AREA 202-CENTRAL	Delaware, District of Columbia, Indiana, Kentucky, Maryland, Ohio, Pennsylvania, Tennessee, Virginia, West Virginia	<ul style="list-style-type: none"> • SB/SE, excluding TS • SB/SE Collec- tions, LB&I and TE/GE shared administrative associates 	Area 202
PROD USER SBSE AREA 203-SOUTH ATLANTIC	Florida, Georgia, North Carolina, South Carolina	<ul style="list-style-type: none"> • SB/SE, excluding TS • SB/SE Collec- tions, LB&I and TE/GE shared administrative associates 	Area 203
PROD USER SBSE AREA 204-MIDWEST	Illinois, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, Wisconsin	<ul style="list-style-type: none"> • SB/SE, excluding TS • SB/SE Collec- tions, LB&I and TE/GE shared administrative associates 	Area 204
PROD USER SBSE AREA 205-GULF STATES	Alabama, Arkansas, Louisiana, Mississippi, Oklahoma, Texas	<ul style="list-style-type: none"> • SB/SE, excluding TS • SB/SE Collec- tions, LB&I and TE/GE shared administrative associates 	Area 205

Exhibit 4.7.2-5 (Cont. 1) (06-27-2022)
ERCS BEARS Applications for SBSE

BEARS ERCS application	Location of User	BOD of User	Access needed for returns in
PROD USER SBSE AREA 206-WESTERN	Alaska, California (Northern), Colorado, Idaho, Montana, Nevada, Oregon, Utah, Washington, Wyoming	<ul style="list-style-type: none"> • SB/SE, excluding TS • SB/SE Collections, LB&I and TE/GE shared administrative associates • SBSE includes groups in the Micro Captive Territory without regard to state 	Area 206
PROD USER SBSE AREA 207-SOUTHWEST	Arizona, California (Southern), Hawaii, New Mexico	<ul style="list-style-type: none"> • SB/SE, excluding TS • SB/SE Collections, LB&I and TE/GE shared administrative associates • SBSE includes groups in the ATTI and R&E Territories without regard to state 	Area 207

Exhibit 4.7.2-6 (06-27-2022)

ERCS BEARS Applications for LB&I

BEARS ERCS application	Location of User	BOD of User	Access needed for returns in
PROD USER LBI 201-NORTH ATLANTIC	Connecticut, Maine, Massachusetts, New Hampshire, New Jersey, New York, Rhode Island, Vermont	<ul style="list-style-type: none"> • LB&I • SB/SE, SB/SE Collections and TE/GE shared administrative associates 	LB&I
PROD USER LBI 202-CENTRAL	Delaware, District of Columbia, Indiana, Kentucky, Maryland, Ohio, Pennsylvania, Tennessee, Virginia, West Virginia	<ul style="list-style-type: none"> • LB&I • SB/SE, SB/SE Collections and TE/GE shared administrative associates 	LB&I
PROD USER LBI 203-SOUTH ATLANTIC	Florida, Georgia, North Carolina, South Carolina	<ul style="list-style-type: none"> • LB&I • SB/SE, SB/SE Collections and TE/GE shared administrative associates 	LB&I
PROD USER LBI 204-MIDWEST	Illinois, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, Wisconsin	<ul style="list-style-type: none"> • LB&I • SB/SE, SB/SE Collections and TE/GE shared administrative associates 	LB&I
PROD USER LBI 205-GULF STATES	Alabama, Arkansas, Louisiana, Mississippi, Oklahoma, Texas	<ul style="list-style-type: none"> • LB&I • SB/SE, SB/SE Collections and TE/GE shared administrative associates 	LB&I
PROD USER LBI 206-WESTERN	Alaska, California (Northern), Colorado, Idaho, Montana, Nevada, Oregon, Utah, Washington, Wyoming	<ul style="list-style-type: none"> • LB&I • SB/SE, SB/SE Collections and TE/GE shared administrative associates 	LB&I
PROD USER LBI 207-SOUTHWEST	Arizona, California (Southern), Hawaii, New Mexico	<ul style="list-style-type: none"> • LB&I • SB/SE, SB/SE Collections and TE/GE shared administrative associates 	LB&I