Correspondence Examination Automation Support (CEAS), Release 2, Milestone 4.b, Version 0.1 Privacy Impact Assessment

PIA Approval Date: Jan. 25, 2007

System Overview

Correspondence Examination Automation Support (CEAS) is a suite of Web-based applications developed to enhance the Campus examination process.CEAS applications satisfy Client & RGS Batch requests to store/retrieve exam cases to/from the CEAS centralized database. CEAS also enables case assignment and transfer between examination groups and batch groups. CEAS facilitates universal view of the campus exam case inventory records and also allows the display of the client generated tax reports and letters associated with the exam case. CEAS has the capability to interface with AIMS, allowing for account reconciliation between CEAS and AIMS campus inventories. Additionally, CEAS supplies a series of reports which assist the various levels of management to control/manage.

Data in the System

1. **Generally describe the information to be used in the system in each of the following categories: Taxpayer, Employee, and Other.**
   Taxpayer:
   Taxpayer information includes several categories, including:
   - Business credits information
   - Business deduction information
   - Business exemption information
   - Business expenses information
   - Business income information
   - Business payment information
   - Taxpayer credits information
   - Taxpayer deduction information
   - Taxpayer exemption information
   - Taxpayer expenses information
   - Taxpayer income information
   - Taxpayer payment information

   Within these categories, CEAS looks at the following fields to perform its function:
   - Assessed tax liability
   - Balance due amounts
   - Business EIN (or other TIN)
   - Business taxpayer address
   - Business taxpayer name
   - Dividends
   - Employment status
   - Gambling winnings
   - Individual SSN
   - Individual taxpayer address
   - Individual taxpayer name
   - Interest income
   - Interest paid
   - IRA contribution
   - Miscellaneous income
   - Other credits

- Payments
- Power of Attorney (PAO)
- Proceeds from real estate transactions
- Proceeds from stock sales
- Refund checks sent
- Student loan interest
- Tax period
- Taxpayer Identification Number (TIN)
- Tuition payments
- Wages earned
- Withholdings

Employee:

- System User ID
- Standard Employee Identifier (SEID)
- Password

Audit Trail Information:

- Date time stamp (e.g., date and time of the event)
- Unique identifier (e.g., user name, SEID, application name, etc.) of the user or application initiating the event)
- Type of event
- Origin of the request (e.g., terminal ID) for identification/authentication of events
- Name of object introduced, accessed, or deleted from a user's address space
- Role of user when creating the event
- Success/Failure of the event

For systems that store or process taxpayer information, audit trail records for the transactions identified above includes the following data elements, where applicable:

- Type of event (e.g., command code)
- Terminal and employee identification
- Date and time of input
- Account accessed to include the TIN
- Master File Tax (MFT)
- Tax period.

Other: None.

2. What are the sources of the information in the system?

2.a. What IRS files and databases are used?

CEAS data inputs:

- Executive Control Program for IMF Extract (IMF 701 EXEC)
- Individual Return Transaction File On-Line Processing (IRTFOL)
- Report Generation Software (RGS).
- Total Interest Program System (TIPS)
- Legacy Access Provider (LAP)
- Security and Communications System (SACS)
- Audit Information Management System (AIMS)

- Discretionary Automated Examination (DAE)
- Dependent Database (DDB)

CEAS data outputs:

- Audit Information Management System (AIMS)
- Examination Operational Automation Database (EOAD)
- Taxpayer Information File (TIF)
- Automated Case Workload Manager (ACWM)

The application environment is located at MITS-3 in Martinsburg, WV (ECC-MTB) and the production environment is located at MITS-4 in Memphis, TN (ECC-MEM). In addition, CEAS replies on:

- MITS-1: IRS Perimeter Security and Network Backbone
- MITS-3: Martinsburg Computing Center (ECC-MTB) Domain
- MITS-4: Tennessee Computing Center (ECC-MEM)/Memphis Campus Domain
- MITS-17: Workstations/Servers controls and support for production, development, and test environments
- MITS-26: Enterprise Remote Access

There are between 3500 to 3600 CEAS users from W&I and SB/SE business units, including managers, tax examiners, clerks, batch coordinators and HQ analysts from all ten IRS campuses:

- MITS-3: Memphis Campus Domain
- MITS-5: Andover Campus Domain
- MITS-6: Atlanta Campus Domain
- MITS-7: Austin Campus Domain
- MITS-8: Brookhaven Campus Domain
- MITS-9: Cincinnati Campus Domain
- MITS-10: Fresno Campus Domain
- MITS-11: Kansas City Campus Domain
- MITS-12: Philadelphia Campus Domain
- MITS-13: Ogden Campus Domain
- MITS-14: National Office Domain

2.b. What Federal Agencies are providing data for use in the system?

None.

2.c. What State and Local Agencies are providing data for use in the system?

None.

2.d. From what other third party sources will data be collected?

None.

2.e. What information will be collected from the taxpayer/employee?

Taxpayer: None.

Employee:

- System User ID
- SEID
- Password

3.a. How will the data collected from sources other than IRS records and the taxpayers be verified for accuracy?

As part of the IT modernization effort, the Correspondence Examination Automation Support (CEAS) system will provide infrastructure support to the existing implementations of the Report Generation System (RGS) and will be the platform phased in to replace RGS as it gets phased out. The CEAS design leverages the IRS Tier II strategy and focuses on centralizing data storage in an Oracle database at the Enterprise Computing Center - Memphis (ECC-MEM). Prior to implementing CEAS at a service center, the service center's RGS case and user data must migrate to the CEAS Oracle database located on a Tier II SUN server at the ECC-MEM. Once the data is migrated to the CEAS Oracle database, users access the case data in CEAS through a menu item within RGS. To have Modify access to cases and reports within CEAS, managers, clerks and examiners must first have access to RGS. CEAS interfaces with RGS thru a layer of code called the Transaction Application Interface (TRANSAPI) which allows the two systems to communicate using HTTP over the IRS Intranet.

Key data items are verified for accuracy, timeliness, and completeness at the time of input. These data fields include:

- Taxpayer Identification Numbers (TIN)
- Dates
- Standardized lists

Some data fields do not validated input in order to allow for free form text to be entered by the user. Some examples of data fields that do not contain validation checks include: action notes, comments, status codes, names, addresses, etc.

A quarterly clean-up process occurs to identify discrepancies in RGS ID Code to the Service Center ID code and orphan data (message not related to Case summary). Refer to the standard operating procedure (SOP) document for additional details.

Users must have a logon to the system and be in the correct group to access the data. They are also controlled at the application level by limiting which menu they can access based on their logon. User access is also limited at the database level by the permissions that the application administrator grants them.

3.b. How will data be checked for completeness?
This information is detailed in the *CEAS Transaction Specifications* document (Version 1.31) dated May 11, 2005.

3.c. Is the data current? How do you know?
Yes. CEAS uses the RGS interface, which automatically pulls the most updated data from the Master File. Information pulled from the Master File and duplicated in the TIF/AIMS database while cases are being audited. This database is updated in real-time where the Master File is updated in weekly cycles.

4. Are the data elements described in detail and documented? If yes, what is the name of the document?
Yes. All data elements are listed in the CEAS database dictionary.

Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

- IRS Users
- Tax Examiners
- System Administrators
- Clerks
- Managers
- Coordinators
- Department Heads
- Operations Managers
- HQ Analysts

Contractors do not hold any roles on the CEAS system.

2. How is access to the data by a user determined?

The Campus-based Administrators have the greatest level of functionality and privileges to the application. Users may have more than one role, in which case the user will have more than one user account and a separate account for each role. Roles are depicted based on the interface mode.

2.a. Are criteria, procedures, controls, and responsibilities regarding access documented?

CEAS users are granted access using a unique username and password given to them after being authenticated onto the application. IRS uses the OL5081 process, where the potential user must complete this form and submit it to the employee's manager (or Functional Security Coordinator) and the system administrator of the application for approval. The employee must meet with the manager to verify all the information and electronically sign the form to receive approval before an email gets automatically sent to the system administrator containing details (permission, role, name) about creating the account.

Contractors receive Minimum Background security clearances and must adhere to same the IRS policies and procedures as IRS employees and must also complete the OL5081 form to gain access to the application. Contractors must receive background investigations when they have unescorted staff-like access to information, systems, data, or facilities for 30 or more days while escorts must be provided if contractors need access under 30 days. Initial security training is required within a maximum of 10 days of appointment for new IRS personnel who are managers, users, or operators of sensitive information systems. Contractor risk levels and background investigations are: Low Risk= NACI, Moderate Risk= NACC, High Risk= BI.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

User access will be restricted according to their roles.

Role: Examiners
Permission: Input action and non-action notes. RGS client and RGSLAN capability or RGS client and CEASLAN capability

Role: Clerk
Permission: Input action and non-action notes. RGS client and RGSLAN capability or RGS client and CEASLAN capability

Role: Manager
Permission: Input action and non-action notes. RGS client and RGSLAN capability or RGS client and CEASLAN capability

Role: Coordinator
Permission: Unlock/reset a user's access to the application

Role: Department Head
Permission: Access to reports menu

Role: Operations Manager
Permission: Access to reports menu

Role: HQ Analyst
Permission: Modify the business rules to change the filter process. Access to reports menu

Role: System Administrators
Permission: Add/modify/delete users, add/modify/delete coordinator, add/modify/delete groups, unlock/reset passwords, and delete cases

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?
Access is restricted according to user roles granted to them after they have gone through the process laid out in Question 2.a. (above, *Access to the Data*) and undergo the proper security training and receive an interim security clearance at the minimum.

5.a. Do other systems share data or have access to data in this system? If yes, explain.

Yes.

- Executive Control Program for IMF Extract (IMF 701 EXEC) – IMF 701 EXEC generates either the Dependent Database (DDB) or the Discretionary/Refund (424) work file used by CEAS which identifies the individuals being examined.
- Individual Return Transaction File On-Line Processing (IRTFOL) – Individual taxpayer return information is retrieved from the Master File as a Return Transaction File (RTF) in either Extended Binary Coded Decimal Interchange Code (EBCDIC) or American Standard Coded Information Interchange (ASCII) format and used in RGS to develop cases.
- Report Generation Software (RGS) – Used to make changes to taxpayer information and generate reports that are sent to the taxpayers. Provides inventory, computations, work papers and correspondence for users as well as an electronic download of RTF return data, electronic upload of assessment and closed case data to AIMS.
- Total Interest Program System (TIPS) – TIPS is a comprehensive interest program, which provides simple and complex interest situations.
- Legacy Access Provider (LAP) – a service used by RGS to retrieve and update taxpayer information requested by RGS applications to Legacy systems.
- Security and Communications System (SACS) – Mostly used by LAP and not directly applicable to CEAS. SACS works behind the scenes to process information used by other systems/applications.

- Audit Information Management System (AIMS) – Used to track cases under audit and undergoes real-time audits where the Master File is updated on a weekly basis.
- Examination Operational Automation Database (EOAD) – provides data to allow tracking of adjustments by issue and enhances the ability to identify specific areas of non-compliance based on Examination results.
- Taxpayer Information File (TIF) via LAP, SACS, and SIA. – Result of system of records for taxpayers.
- Discretionary Automated Examination (DAE) – A selection tool to collect records to be audited.
- Automated Case Workload Manager (ACWM) – CEAS provides inventory levels to ACWM which then requisitions work from the Dependent Database. (No new functionality in this release of CEAS.)
- Dependent Database (DDB)- A selection tool to collect records to be audited.

5.b. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?
Project Management team and user community.

6.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, & Other)?
No. Other states or local taxing agencies may receive data contained in the system indirectly though the EOAD.

6.b. How will the data be used by the agency?
Not applicable.

6.c. Who is responsible for assuring proper use of the data?
The System Administrators assign permissions and are responsible for the proper use of the data.

6.d. How will the system ensure that agencies only get the information they are entitled to under IRC 6103?
Not applicable. CEAS does not share any information directly to other agencies.

<u>Attributes of the Data</u>

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?
Yes. Users need taxpayer information to create and to examine taxpayer returns.

2.a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

Taxpayer: No.
Employee: No.

2.b. Will the new data be placed in the individual's record (taxpayer or employee)?

Taxpayer: Not Applicable.
Employee: Not Applicable.

2.c. Can the system make determinations about taxpayers or employees that would not be possible without the new data?

Taxpayer: No.
Employee: No.

2.d. How will the data be verified for relevance and accuracy?
This information is detailed in the *CEAS Transaction Specifications* document (Version 1.31) dated May 11, 2005.

3.a. If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain.
Master File information is duplicated and stored in the TIF/AIMS database to track cases under Examination.

3.b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
CEAS is a tool that supports W&I and SB/SE divisions by allowing the users to conduct their Examination of tax returns more efficiently. The audit trails and unauthorized access (UNAX) logs are internal systems that tracks the work of users for management reasons and this functionality supports the business purpose of the system.

Audit trails will be used to record the actions taken by individuals or groups. Users must agree to the requirements stated in a banner/system use notification that is displayed prior to them accessing the application.

4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.
Users will access the data through a menu item within RGS thru a layer of code called the Transaction Application Interface (TRANSAPI), which allows the two systems to communicate using HTTP over the IRS Intranet. The LAP server acts as a gateway to allow CEAS real-time access to TIF/AIMS and CFOL data. The CEAS system will use this server to retrieve and update taxpayer information as requested by the CEAS and RGS workstation applications. Users can search the system using any part of personally identifiable elements to filter through records and isolate cases.

Users can only access opened cases assigned to them or self-assigned open cases on a need-to-know basis and are restricted according to their role or function performed.

Taxpayer Identification Numbers (TIN) can be used to verify key data for accuracy, timeliness, and completeness at the time of input. TINs are also used in audit trails. However, users cannot access IRS employee TINs.

5. What are the potential effects on the due process rights of taxpayers and employees of:

None.

a. **Consolidation and linkage of files and systems;**
   Taxpayer: None.
   Employee: None.

b. **Derivation of data;**
   Taxpayer: None.
   Employee: None.

c. **Accelerated information processing and decision making;**
Taxpayer: None.
Employee: None.

d. **Use of new technologies:** None.

How are the effects to be mitigated? Not Applicable.

Maintenance of Administrative Controls

1.a. Explain how the system and its use will ensure equitable treatment of taxpayers and employees.
CEAS interfaces through RGS to provide centralization and automation of the Examination process by enabling IRS-wide database access over the intranet. Taxpayer information is automatically pulled from the Master File (IRTFOL) in the form of reports and queries.

1.b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites?
The application is accessed securely over the Local Area Network (LAN) and the Wide Area Network (WAN) (or through a Virtual Private Network (VPN) when using Enterprise Remote Access Project (ERAP)) and will expedite centralized case management to increase the number of correspondence Examination cases that can be processed within the W&I and SB/SE business units.

Enterprise Technical Support Services (ETSS), in conjunction with Information Technology Infrastructure (ITI), will be responsible for:

- Providing sufficient computer hardware resources and software to effectively operate and properly maintain the CEAS application;
- Controlling, installing and tuning hardware, operating systems, and Commercial Off-the-Shelf (COTS) software (coordinating with Distributing Systems Management Branch (DSMB), the development site (ECC MTB) and the operational site (ECC MEM);
- Monitoring system usage during and after the implementation period and making any changes to the volume forecasts to help in capacity planning, as cited in the SSP for this Application (Version 0.2, dated December 08, 2006);
- Helping monitor system capacity (disk usage, processors, and memory and response time optimization) to prevent user response-time problems or downtime.

1.c. Explain any possibility of disparate treatment of individuals or groups.
Users must access taxpayer information to develop and examine tax returns.

Employee information is needed when filing the OL5081 to attain User ID and passwords and to give users certain permissions to limit their roles.

Audit trails are necessary to ensure accountability and maintain system security.

2.a. What are the retention periods of data in this system?
IRS systems (including applications, databases, network devices, and operating systems), which are not covered by the scope of a system records retention schedule go by the default log retention policy:

- Online computer audit logs are retained for 2 days prior to archival.
- Archival logs are retained for a minimum of 6 months.
- An Information System Owner may establish a system-level business requirement to retain online or archival logs for a longer period than the minimums specified above. The amount of time that the system-level business wants to retain logs should be placed in the Audit Plan.
- IRS organizations or individuals (such as System Administrators) that desire shorter minimum log retention periods than those specified above must submit a Deviation request to justify the shorter retention period.

Database audit data is not required to be local to the database for the period of retention, but is available for historical analysis if needed. Audit data is only readable by personnel authorized by the Security Specification, which ensures that the Database Management System (DBMS) transaction logs are reviewed weekly or more frequently for suspicious or unauthorized changes to sensitive data.

At the end of the retention period, the audit logs are reviewed to determine if the logs require archival at the Federal Records Center or destruction. IRM 10.8.3, Audit Logging Security Standards specifies that archival logs shall be retained for six (6) years, unless otherwise specified by a formal Records Retention Schedule developed in accordance with IRM 1.15, Records Management.

2.b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?
CEAS automatically produces hardcopy letters for filing, which are filed in Return Files according to IRM 1.52.2, *Records Management*, dated January 1, 2003. Electronic case data storage occurs on a near-line unit (Clarion SAN).

IRS follows disk sanitization procedures for destruction of discarded media, according to IRM 2.7.4.

2.c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?
If the data contains personally identifiable information, then the UNAX log files will be kept indefinitely.

Audit trails that store or process taxpayer information is retained in archival logs and retained for 6 years, unless otherwise stated by a formal Records Retention Schedule established in IRM 15.1, *Records Management*. Audit logs may be retained for up to 7 years, per IRM 1.15, which has precedence over IRM 15.1 for systems covered by IRM 1.15

3.a. Is the system using technologies in ways that the IRS has not previously employed (e.g. Caller-ID)?
No. CEAS is using existing technologies, to connect users across the ten IRS Campuses to increase efficiency and coordination. Before, users were unable to automatically share information regarding their cases with other users in difference Campuses.

3.b. How does the use of this technology affect taxpayer/employee privacy?
There is no new technology. Taxpayer/Employee privacy will not be affected in any new way.

4.a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
Yes. Users access taxpayer information to develop and examine tax returns.

Employee information is needed when filing the OL5081 to attain User ID and passwords and to give users certain permissions to limit their roles.

Audit trails are necessary to ensure accountability and maintain system security.

4.b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.
No.

4.c. What controls will be used to prevent unauthorized monitoring?
CEAS uses Java and .NET functionality (garbage collection) that prevents unauthorized and unintended information transfer via shared system resources. "Garbage collection" is a term used to describe how objects are destroyed in an effort to keep others from reusing them.

UNAX logs are kept indefinitely and available for review when there is a suspected violation.

5.a. Under which Systems of Record Notice (SORN) does the system operate? Provide number and name.

- Treasury/IRS 34.037 – IRS Audit Trail and Security Records System
- Treasury/IRS 42.001 – Examination Administrative File

5.b. If the system is being modified, will the SORN require amendment or revision? Explain
No.

View other PIAs on IRS.gov