**Enterprise Forensics and eDiscovery (EnCase) – Privacy Impact Assessment**

**PIA Approval Date – Mar. 14, 2011**

## System Overview

The Enterprise Forensics and eDiscovery (EnCase) solution is a major application that has been procured by, and is currently under deployment by the Internal Revenue Service (IRS) supported by the Modernization and Information Technology Services (MITS), Office of Cybersecurity Program and Policy. The Internal Revenue Service is confronting a constantly changing threat environment – increasingly sophisticated system intrusion attempts and potential for data leakage, rising malware threats, and inconsistent forensic analysis and threat mitigation procedures and enforcement. System and Network threat issues Office of Management and Budget (OMB, memorandum OMB M–0622) and are outlined in the new Cybersecurity Initiative. By nature of its activities and high visibility, the IRS is an obvious target for cyber attacks and network threats. The information collected and managed by the IRS is of extremely high value for the agency, the Treasury Department, and the U.S. population. Therefore, the comprehensive Cybersecurity forensic system and eDiscovery solution, EnCase, is required to control and limit threats to the systems that contain vital information.

## Data in the System

**1. Generally describe the information to be used in the system in each of the following categories:**

A. Taxpayer – Information contained on IRS computers, workstations, laptops, servers and any removable media. Information on these devices consist of:

- Taxpayer name (and spouse)
- Taxpayer address (and spouse)
- Taxpayer identification number (TIN) (and spouse)
- Tax period Liability amount for each tax period Terms of the offer
- All email transmissions
- Litigation information

B. Employee – Employee data used in this system consists of data collected on IRS computers, workstations, laptops, servers, and any removable media. This information includes USERID and password.

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

Information searched and collected by the EnCase system is provided by the IRS employee computers, workstations, laptops, servers, and any removable media. Standard IRS Forms for an EDR (eDiscovery Request) is submitted as part of the process to commence searching of the data. For threat mitigation using EnCase CyberSecurity, the solution commences search and mitigation automatically at initial threat detection.

A. IRS – What IRS files and databases are used?
The EnCase system uses a SQL database that resides on an SQL server located at the IRS facility. The Examiner is Software installed on an authorized investigator's computer to perform incident response, investigations and audit target systems and will reside at various locations. The SAFE communicates with Examiners and targets nodes using 128–bit AES encryption to protect communication between components. The servlet is a nonintrusive, auto–updating, passive piece of software installed on workstations and servers to analyze suspect computers. Connectivity is established between the SAFE, Servlet and the Examiner to analyze and

acquire devices that have the EnCase Servlet installed. Servlets run on the following operating systems: all Windows operating systems, Linux kernel 2.2 and above with Process File System (procfs), Solaris 8/9 (32– and 64–bit), Solaris 8 and 9 (32– and 64–bit), AIX 4.3, 5.1, 5.2 and 5.3 (32– and 64–bit), OSX 10.2+, and Novell NetWare 5.1 SP8, 6.0 SP4 and 6.5.

B. Taxpayer/Employee – What information will be collected from the taxpayer/employee?
Any electronic data transmitted can be collected from the taxpayer/employee.

C. Other Federal Agencies – What Federal Agencies are providing data for use in the system?
The IRS and Treasury are providing data captured by the EnCase system.

**3. How will data collected from sources other than IRS records and the taxpayers be verified for accuracy?**
Not applicable. EnCase does not collect information from sources other than IRS records or taxpayers.

- **How will data be checked for completeness?**
  Not applicable. EnCase does not collect information from sources other than IRS records or taxpayers.

- **Is the data current? How do you know?**
  Not applicable. EnCase does not collect information from sources other than IRS records or taxpayers.

**4. Are the data elements described in detail and documented? If yes, what is the name of the document?**
Data elements for EnCase are described in the EnCase Requirements Document referred to as Business Systems Requirements Report (BSRR).

**Access to the Data**

**5. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?**
EnCase users that capture data in the field offices will consist of designated IRS personnel that deploy the application for CyberSecurity and eDiscovery related tasks.
All IRS personnel who have access to EnCase will have organization specified clearances and are only granted access when their jobs require it. Their access is immediately revoked when it is no longer required.

**6. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**
Access to the data within the system is restricted to the EnCase Examiner. The EnCase Examiner will have access to any and all data pertinent to a set search criteria. Procedures and controls are documented in the EnCase User Manual. The user's profile and roles are assigned by his/her manager which is reviewed 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 EnCase. Criteria, procedures, controls, and responsibilities regarding access are documented in IRS access control documentation.

**7. Will users have access to all data on the system or will the user's access be restricted?**
The Administrator of the Examiner has a need–to–know 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 EnCase. The criteria, procedures, controls and responsibilities regarding access are documented in the IRS access control documentation.
EnCase stores information protected under the Privacy Act of 1974. Such information is categorized as SBU. In addition, the Commissioner of the IRS has designated that all IRS systems and associated data be categorized as SBU, and protected under IRC 6103, Confidentiality and Disclosure of Return and Return Information. Risk Assessments have been performed in accordance with the following guidelines:

- IRM 2.1.10--Information Systems Security, April 30, 1998.
- TD P 71–10--Security Manual, October 1, 1992.
- TD P 85–03--Risk Assessment Guideline, June 1999.
- CSC–STD–003–85--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (TCSEC).

**8.What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?**
EnCase uses audit trails as required by IRS 2.1.10, Information Systems Security, May 1998, and a Functional Security Coordinator is assigned. All employees are required to attend UNAX Training and they have been trained on the use of the system and their responsibilities concerning access and use of the data. The following mandatory rules are defined for users of IRS computer and information systems:

- Users are forbidden to access, research, or change any account, file, record, or application that is not required to perform official duties.
- Users are restricted to accessing, researching, or changing only accounts, files, records, or applications that are required to perform their official duties.
- Users are restricted from accessing their individual/spouse account, accounts of relatives, friends, neighbors, or any account in which the user has a personal or financial interest. Users are restricted from accessing the accounts of a famous or public person unless given authorization to do so.
- If asked to access an account or other sensitive or private information, users are required to verify that the request is authorized and valid.

**9. Do other systems share data or have access to data in this system?**
EnCase does not receive any downloads or extract any data from any other source other than data input directly by tax examiners. Other systems do not electronically access the data within AOIC.

- **Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?**
  The IRS is responsible for protecting the privacy rights of taxpayers and employees regarding data contained within EnCase.

**10. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?**
No other agencies share data or have access to the data contained in or transmitted by EnCase.

- **How will the data be used by the agency?**
  No other agencies share data or have access to the data contained in or transmitted by EnCase.
- **Who is responsible for assuring proper use of the data?**
  No other agencies share data or have access to the data contained in or transmitted by EnCase.
- **How will the system ensure that agencies only get the information they are entitled to under IRC 6103?**

No other agencies share data or have access to the data contained in or transmitted by EnCase. The only external agencies granted access to EnCase are the Treasury Inspector General for Tax Administration (TIGTA) and the General Accounting Office (GAO). Access is granted for auditing purposes and only for the amount of time required for the audit. Information within the system will not be disclosed except as expressly authorized by IRC 6103.

## Attributes of the Data

**11. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**
Yes. The data used in EnCase is both relevant and necessary to the purpose for which the system has been designed.

**12. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?**
The data derived from EnCase will be used for litigation purposes, and any and all data retrieved can be used to support litigation (or potential litigation) proceeding. EnCase does not derive or create previously unavailable data about an individual through aggregation from the information collected.

- **Will the new data be placed in the individual's record (taxpayer or employee)?**
  EnCase does not derive or create previously unavailable data about an individual through aggregation from the information collected.
- **Can the system make determinations about taxpayers or employees that would not be possible without the new data?**
  EnCase cannot make determinations about taxpayers or employees.
- **How will the new data be verified for relevance and accuracy?**
  EnCase does not derive or create previously unavailable data about an individual through aggregation from the information collected.

**13. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**
Information retrieved by EnCase is not consolidated, changed, or modified in any way.

- If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain
  Information retrieved by EnCase is not consolidated, changed, or modified in any way.

**14. How will the data be retrieved? Can it be retrieved by personal identifier?**
Files can be retrieved by taxpayer name, case number, or any other given search criteria.

- **What are the potential effects on the due process rights of taxpayers and employees of:**
  - consolidation and linkage of files and systems;
    EnCase does not consolidate processes or link files
  - derivation of data;
    Data is derived from the employee laptops, workstations, and server, and any removable media.
  - accelerated information processing and decision making;
    The accelerated information processing performed by the EnCase system does not affect the due process rights of the taxpayers or employees. EnCase does not perform any decision–making.
  - use of new technologies;
    EnCase does not affect the due process rights of taxpayers or employees.

- **How are the effects to be mitigated?**
  EnCase does not affect the due process rights of taxpayers or employees.

**Maintenance of Administrative Controls**

**15. Explain how the system and its use will ensure equitable treatment of taxpayers and employees.**
The EnCase System allows for inventory control, data analysis, automated internal transaction processing, and automated standardized letter/form processing.
System management is responsible for the proper operation of the system, ensuring correct processing and responses to users, as well as the oversight of employees' use of the system and the data contained therein.

- **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**
  EnCase is housed at IRS locations and data center.
- **Explain any possibility of disparate treatment of individuals or groups.**
  EnCase is a search and forensics tool for Cybersecurity and eDiscovery. There is no possibility of disparate treatment of individuals or groups. All taxpayers are treated equally. The IRS allows supervisors and reviewers to monitor examiners and specialists decisions to ensure that taxpayers are being treated fairly according to their individual circumstances. It also allows examiners and specialists to research decisions made in similar cases.

**16. What are the retention periods of data in this system?**
Data records are maintained in accordance with IRM 1.15.

- **What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?**
  Data records are maintained in accordance with IRM 1.15.
- **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?**
  The data retention period for data captured by EnCase is 10 years.

**17. Is the system using technologies in ways that the IRS has not previously employed (e.g., Caller–ID)?**
EnCase is not using technologies in ways that the IRS has not previously employed.

- **How does the use of this technology affect taxpayer/employee privacy?**
  EnCase is not using technologies in ways that the IRS has not previously employed.

**18. Will this system provide the capability to identify, locate, and monitor individuals?**
Yes. Information retrieved from EnCase can contain individual taxpayer information such as name, address, and taxpayer identification number.

- **Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.**
  Yes. Information retrieved by EnCase can contain individual taxpayer information such as name, address, and taxpayer identification number.
- **What controls will be used to prevent unauthorized monitoring?**
  Only authorized employees have access to the information on EnCase. All employees and contractors receive UNAX and Code of Conduct training. Identification and access provisions are employed.

**19. Under which Systems of Record Notice (SOR) does the system operate? Provide number and name.**

Not applicable.

**View other PIAs on IRS.gov**