Cybercrime Investigation System (CIS)
Privacy Impact Assessment (PIA)

Date of Submission: 07/25/2011

Contact Information:

James Jackson, Special Agent in Charge, Electronic Crimes, and Intelligence Division, ECID, 202.283.2122, James.Jackson@tigta.treas.gov

Keith Kratzer, Chief Information Security Officer, OMS, 770.452.4001, Keith.Kratzer@tigta.treas.gov

Margaret (Micki) Martin, Acting Chief Counsel, OCC, 202.622.7564, Margaret.Martin@tigta.treas.gov

1. What is the purpose of the system/application?

The Cybercrime Investigation System (CIS) is comprised of equipment maintained by the Cybercrime staff and the OS X systems used by both Cybercrimes and Digital Forensic Support (DFS) agents. The equipment maintained by the CIS staff is used exclusively for Law Enforcement activities. It stores evidence for investigative cases and is used to research casework and examine and analyze evidence.

This system contains varying information on individuals depending on the purpose of the investigation. The information may contain any combination of specific identifiable information such as name, SSN, phone number, or address. The nature and scope of ECID pertains to the enforcement of criminal laws which may exempt the Cybercrimes system from certain provisions of the Privacy Act of 1974, Public Law 93-579, as provided for by 5 U.S.C. §552a(j)(2) and 5 U.S.C. §552a(k)(2).

2. What legal authority authorizes the purchase or development of this system/application?

The TIGTA Office of Investigations (OI), Electronic Crimes and Intelligence Division (ECID) is composed of three distinct functional areas which deal with investigating crimes and researching and collecting criminal intelligence information in an electronic environment. As such, ECID is routinely required to collect and analyze electronic evidence from both Internal Revenue Service (IRS) and non-IRS computer systems, download and analyze malicious code and other software programs associated with ongoing investigations, as well as conduct in-depth Internet research related to both electronic and physical threats to IRS employees and other critical IRS physical and network infrastructure.

The Cybercrimes system is the system infrastructure that ECID personnel use to perform their day-to-day duties which provides data access and Internet services. The data/information obtained is used by ECID's personnel for investigative purposes and is necessary to identify and prevent fraud, waste, and abuse in the programs and operations of the IRS and related entities as well as to promote economy, efficiency, and integrity in the administration of the internal revenue laws and detect and deter wrongdoing by IRS and TIGTA employees or contractors. The specific data elements consist of extracts from various electronic systems maintained by governmental agencies and other entities that will be used vary depending on the unique needs of each investigation which can include personal information on individuals.

The nature and scope of TIGTA's oversight and investigative responsibilities were established and set forth in the Inspector General Act of 1978, as amended, (I.G. Act), 5 U.S.C Appendix 3 and Treasury Order 115-01. In order to enable TIGTA to perform its oversight and investigative functions, the I.G. Act authorizes TIGTA to have access to "all records, reports, audits, reviews, documents, papers, recommendations, or other material" maintained by the IRS. In addition, both the Privacy Act and I.R.C §6103(h)(1) authorize TIGTA to receive information for purposes of performing its official responsibilities.

3. Under which Privacy Act SORN does the system operate? (Provide the system name and unique system identifier.)

Treasury/DO.311, TIGTA Office of Investigations Files, 75 F.R. 75 (April 20, 2010)

4. What categories of individuals are covered in the system?

The following are categories of individuals covered in the system:

- The subjects or potential subjects of investigations
- The subjects of complaints received by TIGTA

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

Information for investigations and complaints comes from multiple sources. The original complaint or accusation comes from an individual. Based on this initial information, other case-related information may come from the following sources:

- Social Security Administration Account Data
- Treasury FMS Treasury Checks
- Informants and Confidential Sources
- Law Enforcement Databases
- Treasury Enforcement Communications System (TECS).
- National Crime Information Center (NCIC).
- National Law Enforcement Telecommunication System (NLETS).

- El Paso Intelligence Center (EPIC).
- Information from State or US Territorial Taxing Authorities

Some records contained within this system are exempt from the requirement that the record source categories be disclosed pursuant to the provisions of 5 U.S.C 552a (j)(2) and (k)(2). Non-exempt source categories include the following: Department of the Treasury personnel and records, complaints, witnesses, governmental agencies, tax returns and related documents, subjects of investigations, persons acquainted with the individual under investigation, third party witnesses, Notices of Federal Tax Liens, court documents, property records, newspapers and periodicals, financial institutions and other business records, medical records, and insurance companies.

6. How will data collected from sources other than bureau records be verified for accuracy, timeliness, and completeness?

The data/information obtained and stored in Cybercrimes system is used by ECID's personnel for investigative purposes, and it is their responsibility to perform comprehensive analyses to verify data for accuracy, timeliness, and completeness. The investigative process is designed to meet certain legal standards and the process verifies data for accuracy, timeliness, and completeness with a greater degree of certainty than traditional administrative requirements.

7. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

The Cybercrimes system is the system infrastructure which provides data access and Internet services that ECID personnel use to perform their day-to-day duties. The data/information obtained is used by ECID's personnel for investigative purposes and is necessary to identify and prevent fraud, waste, and abuse in the programs and operations of the IRS and related entities as well as to promote economy, efficiency, and integrity in the administration of the internal revenue laws and detect and deter wrongdoing by IRS and TIGTA employees or contractors. The specific data elements consist of extracts from various electronic systems maintained by governmental agencies and other entities the use of which varies depending on the unique needs of each investigation.

8. What are the retention periods of data in this system?

Not applicable. When the investigation is over, and the specific data collected is no longer needed on the system, the case agent is responsible for disposing the data

9. Will this system provide the capability to identify, locate, and monitor individuals? **If yes, explain**.

Yes. The data/information stored in Cybercrimes system is used by ECID's personnel for investigative purposes which allows them to perform comprehensive analyses of employee, taxpayer, and tax administration data necessary to identify and prevent fraud, waste, and abuse in the programs and operations of the IRS and related entities as well as to promote economy, efficiency, and integrity in the administration of the internal revenue laws and detect and deter wrongdoing by IRS and TIGTA employees or contractors.

10. What controls will be used to prevent unauthorized monitoring?

TIGTA Security Rules of Behavior state: "Do not access, research, or change any account, file, record, or application not required in performing your official duties." TIGTA employees should always verify that the request of accessing data has been authorized. All TIGTA employees are required to undergo yearly security, privacy, and ethics training. System access is monitored closely and if a user or an administrator violates the organization's security policies he/she may be subject to disciplinary action, up to and including termination of employment

11. Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, others)

Cybercrimes is an internal system that is not accessible by the public. The Cybercrimes system contains sensitive data that needs to be protected and guarded to the maximum extent possible. ECID's personnel who have been granted access to the system are responsible for providing the level of protection warranted by the classification of the information and material in his or her possession or control.