United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf.

If you need further assistance contact Marlyn Aguilar, at aguilar.marlyn@epa.gov or (202) 566-0012.

System Name: OCEFT Criminal Investigative Index and Files (Criminal Case Report System – CCRS)	
Preparer: Eric Blank	**Office: OECA/OCEFT/CID**
Date: May 21, 2018	**Phone: 202-566-0656**
Reason for Submittal: New PIA____ Revised PIA____ Annual Review__X__ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐	
Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).	
The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).	

Provide a general description/overview and purpose of the system:

To support and further the investigation of persons or organizations alleged to have criminally violated any environmental statute or regulation. Criminal violations of other federal statures may have occurred in conjunction with such environmental violations and therefore, may also be within the scope of an OCEFT/CID investigation and may be included in the record system.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the system in question?

18 U.S.C. 3063; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9603; Resource Conservation and Recovery Act, 42 U.S.C. 6928; Federal Water Pollution Control Act, 33 U.S.C. 1319, 1321; Toxic Substances Control Act, 15 U.S.C. 2614, 2615; Clean Air Act, 42 U.S.C. 7413; Federal Insecticide, Fungicide and Rodenticide Act, 7 U.S.C. 136j, 136l;

Safe Drinking Water Act, 42 U.S.C. 300h-2, 300i-1; Noise Control Act of 1972, 42 U.S.C. 4912; Emergency Planning and Community Right-To-Know Act of 1986, 42 U.S.C. 11045; and the Marine Protection, Research, and Sanctuaries Act of 1972, 33 U.S.C. 1415.

1.2 Has a system security plan been completed for the information system(s) supporting the system?

Yes

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

CCRS is not covered by the Paperwork Reduction Act (PRA

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

Name, Address, Telephone Number, Employee ID, Personal Cell Phone Number, Home Email, Date of Birth, Fax Numbers, Driver's License Number, Case ID Number, Social Security Number

2.2 What are the sources of the information and how is the information collected for the system?

The information collected in CCRS includes investigative activity reports, investigative summary reports, subject information, and sentencing information. The information is obtained as a result of various investigative activities, including tips, complaints, interviews, surveillance, records review, evidence collection and analysis, and judicial action. The data is used to document the progress and results of criminal investigations.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No

2.4 Discuss how accuracy of the data is ensured.

Review of data for quarterly stats.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

PII such as Name, Address, Telephone Number, Employee ID, Personal Cell Phone Number, Home Email, Date of Birth, Fax Numbers, Driver's License Number, Case ID Number, Social Security Number. Printing or other unauthorized sharing of information is a risk.

Mitigation:

Several layers including the agency network security process, NCC controls, CCRS roles which control access to these items, and data entry process.

Records management procedures, including security clearances, training, and code of conduct. This includes PL-4 – Rules of Behaviors, CIO 2151.1 - Privacy Policy, and CIO 2150-P-21.0 – Information Security – National Rules of Behavior.

Section 3.0 Uses of the Information

The following questions require a clear description of the system's use of information.

3.1 Describe how and why the system uses the information.

The agency uses this information to identify suspects, witnesses, and victims in the course of an investigation.

To the extent permitted under the Privacy Act of 1974, 5 U.S.C. 552a(j) (2) or (k)(2), this system has been exempted from the provisions of the Privacy Act of 1974 that permit access and correction. Exemptions from access may be complete or partial, depending on the exemption applicable. However, EPA may, in its discretion, grant individual requests for access and correction if it determines that the exercise of these rights will not interfere with an interest that the exemption is intended to protect.

- To support and further the investigation of persons or organizations alleged to have criminally violated any environmental statute or regulation. Criminal violations of other federal statutes may have occurred in conjunction with such environmental violations and, therefore, may also be within the scope of an OCEFT/CID investigation and may be included in the record system.

3.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X__ No___. If yes, what

identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

Lead and case files are assigned unique system generated numbers and a name created by the agent, which could be the suspect's name. Individuals and companies related to cases and leads are primarily identified by their name and, if needed, other identifiable information such as age, race, sex, address, etc.

3.3 If the system retrieves information by personal identifier, what types/elements of information about the user are being retrieved?

Information is retrieved by OCEFT/CID case number or the case name. The case name may be either a company name or the name of a person that denotes the subject of the investigation.

3.4 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

OCEFT Criminal Investigative Index & File. SORN Number EPA-17

3.5 Does the system use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how EPA plans to use such results.

No

3.6 <u>Privacy Impact Analysis</u>: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

<u>Privacy Risk</u>:

None

<u>Mitigation</u>:

None

Section 4.0 Notice

The following questions seek information about the system's notice to the individual about the

information collected, the right to consent to uses of information, and the right to decline to provide information.

4.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

No, because the data involves ongoing criminal investigations.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

Any individual who wants to know whether this system of records contains a record about him or her, who wants access to his or her record, or who wants to contest the contents of a record, should make a written request to the Freedom of Information Office. Requesters will be required to provide adequate identification, such as a driver's license, employee identification card, or other identifying document. Additional identification procedures may be required in some instances.

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are set out in 40 CFR part 16.

4.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

The data we collect is only as accurate as what an agent is given during the case. An agent can change the data in a case throughout the lifecycle of a case. Therefore, privacy oriented data may be changed.

Mitigation:

Agents strive to be accurate in their casework. Data entry is manual, there is no

automated quality assurance.

Section 5.0 Access and Data Retention by the system

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

5.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

The system uses a combination of Security Roles (e.g. Supervisor, Agent, No CCRS Access, etc) and Position (e.g. Special Agent in Charge, Special Agent, Administrative Specialist, etc) for access control.

5.2 Are there other components with assigned roles and responsibilities within the system?

Yes

5.3 Who *(internal and external parties)* will have access to the data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

EPA Internal Use Only

Access is granted to OECA/OCEFT/CID Personnel

Contract through Leidos to maintain the system the contract number is HHSN316201200034W.and the contract has the following FAR Clause in it FAR 52.232-8, Federal Acquisition Regulation (FAR) Subpart 42.15, FAR 31.205-43, FAR 31.205-46, FAR 52.252-2, FAR 52.209-5, FAR 52.209-7, FAR 52.209-9, FAR 52.217-5, FAR 52.217-8, FAR 52.217-9, FAR 52.224-1, FAR 52.224-2, FAR 52.232-25, FAR 52.232-33, FAR 52.232-99, FAR 52.237-3, FAR 52.239-1, FAR 52.249-4, and FAR 52.253-1

5.4 What procedures are in place to determine which users may access the information and how does the system determine who has access?

Through roles, depending on job titles and location.

5.5 Explain how long and for what reason the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

EPA Records Schedule 0684 **http://intranet.epa.gov/records/schedule/final/0684.html**

5.6 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes

5.7 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align with the stated purpose and mission of the system.

Privacy Risk:

Retention and Disposal: The manner of Retention and Disposal of the computer index and files depends on how the information is used. The files and computerized data fall into one of three categories:

1. For cases investigated but not referred to the Department of Justice (DOJ) for criminal prosecution, files are retained in the applicable OCEFT/CID office for two years after the investigation is closed and then forwarded to the Federal Records Center (FRC) nearest the System Location for an additional three years. The FRC will normally destroy the files after three years.
2. For cases referred to DOJ but DOJ declines to prosecute, files are retained by the applicable OCEFT/CID office for five years after DOJ declines to prosecute and then retired to the FRC, where they are normally destroyed after five years.
3. For cases that become the subject of judicial action, files are retained by the applicable OCEFT/CID office for five years after completion of the judicial action and then forwarded to the FRC for an additional ten years of retention. The FRC normally destroys the case files after ten years.

Mitigation:

Several layers including the agency network security process, NCC controls, CCRS roles which control access to these items, and data entry process.

Records management procedures, including security clearances, training, and code of conduct. This includes PL-4 – Rules of Behaviors, CIO 2151.1 - Privacy Policy, and CIO 2150-P-21.0 – Information Security – National Rules of Behavior.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

6.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

Yes

General Routine Uses A, C, D, E, F, G, H, and K apply to this system. Records may also be disclosed:

1. To a potential source of information to the extent necessary to elicit information or to obtain cooperation of that source in furtherance of an EPA criminal investigation.
2. To the Department of Justice for consultation about what information and records are required to be publicly released under federal law.
3. To a federal agency in response to a valid subpoena.
4. To Federal and state government agencies responsible for administering suspension and debarment programs.
5. To international law enforcement organizations if the information is relevant to a violation or potential violation of civil or criminal law or regulation within the jurisdiction of the organization or a law enforcement agency that is a member of the organization.
6. To the news media and public unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of privacy.
7. To any person if the EPA determines that compelling circumstances affecting human health, the environment, or property warrant the disclosure.
8. In connection with criminal prosecution or plea negotiations to the extent that disclosure of the information is relevant and necessary to the prosecution or negotiation and except where court orders are otherwise required under section (b)(11) of the Privacy Act of 1974, 5 U.S.C. 552a(b)(11).

6.2 Describe how the external sharing noted in 6.1 is compatible with the original purposes of collection in the SORN noted in 3.4.

External sharing is compatible with the SORN because it meets our requirements to share our cases with DOJ and FOIA requests.

6.3 Does the agreement place limitations on re-dissemination?

All documents contain the following paragraph:

"This document contains neither recommendations or conclusions of the EPA. It is the property of the EPA and is loaned to your agency; it and its contents are not to be distributed outside your agency."

6.4 Describe how the system maintains a record of any disclosures outside of the Agency.

For FOIA requests there's a database called FOIAonline. More information can be found here: http://intranet.epa.gov/foia/

Referrals to DOJ are handled through Investigative Activity Reports.

6.5 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

Users are required to sign a CCRS Access Request form, which contains the following statement:

I read and I understand the CCRS Rules of Behaviors pertaining to my Criminal Case Reporting System responsibilities. I will abide by these rules and understand that failure to comply with them may be grounds for disciplinary action.

These are the CCRS Rules of Behavior:

https://oasext.epa.gov/ccrs/images/Appendix_A_Rules_of_Behaviors.pdf

6.6 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

None. Information is not shared outside of EPA

Mitigation:

None

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

To the extent permitted under the Privacy Act of 1974, 5 U.S.C. 552a(j)(2) or (k)(2), this system has been exempted from the provisions of the Privacy Act of 1974 that permit access and correction. Exemptions from access may be complete or partial, depending on the particular exemption applicable. However, EPA may, in its discretion, grant individual requests for access and correction if it determines that the exercise of these rights will not interfere with an interest that the exemption is intended to protect.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are set out in 40 CFR part 16.

7.3 How does the system notify individuals about the procedures for correcting their information?

Any individual who wants to know whether this system of records contains a record about him or her, who wants access to his or her record, or who wants to contest the contents of a record, should make a written request to the Freedom of Information Office. Requesters will be required to provide adequate identification, such as a driver's license, employee identification card, or other identifying document. Additional identification procedures may be required in some instances.

7.4 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

None

Mitigation:

None

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the system ensure that the information is used in accordance with stated practices in this PIA?

Several layers including the agency network security process, NCC controls, CCRS roles which control access to these items, and data entry process.

Records management procedures, including security clearances, training, and code of conduct. This includes PL-4 – Rules of Behaviors, CIO 2151.1 - Privacy Policy, and CIO 2150-P-21.0 – Information Security – National Rules of Behavior.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

This training has been conducted via annual IT Security Awareness Training

8.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Staff changes

Mitigation:

Review current CCRS employees and compare to HR roles every quarter.