United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official. ***All entries must be Times New Roman, 12pt, and start on the next line.*** If you need further assistance, contact your LPO. A listing of the LPOs can be found here: https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: Online Criminal Enforcement Activities Network—OCEAN EPA-17	
Preparer: Christopher Prince	**Office:** OECA/OCEFT/CID
Date: February 13, 2024	**Phone:** 202-564-6096
Reason for Submittal: New PIA___ Revised PIA_____ Annual Review____ X ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance X☐ 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, further, and document the investigation of persons or organizations alleged to have criminally violated any environmental statute or regulation, and the discovery and referral to the Office of Inspector General for investigation of threats made to the EPA Administrator or any other EPA senior executive service manager, or their family members. Criminal violations of other federal statutes may have occurred in conjunction with environmental violations, and therefore may also be within the scope of an OCEFT/CID investigation, and records related to such violations may be included in the record system. Any leads and related documents regarding threats to the EPA Administrator, other senior executive service managers, or their family members. may be included in the record system.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) 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. Title 18 Criminal Investigations.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

The Online Criminal Enforcement Activities Network has an ATO. It will expire on October 26, 2025.

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.

No ICR required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes, it will be maintained in the Cloud. MicroPact is the CSP and is FedRamp approved. MicroPact is providing SaaS.

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 OCEAN includes investigative activity reports, investigative summary reports, subject information, sentencing information, and records of or relating to threats to the EPA Administrator, other senior executive service managers, or their family members. The information related to criminal investigation is obtained as a result of various investigative activities, including tips, leads, complaints, interviews, surveillance, records review, evidence collection and analysis, and judicial action. The information related to threats is solicited through open-source search online. 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.

The information has a large variety of sources. It contains information on subjects, witnesses, etc. involving environmental or other federal crimes. Some of it can come from commercial sources (such as Thomson Reuters CLEAR, LexisNexis Accurint, and other data aggregators). It can also come from publicly available sources (new reports, company websites, etc.) The purpose of all the data is to track criminal investigations by the Special Agents, as well as their managers, HQ, etc.; or to document relevant threats and threat referrals to the Office of Inspector General for investigation.

2.4 Discuss how accuracy of the data is ensured.

Review of data for quarterly stats. In addition, managers review the work of their reports to ensure accuracy as well as timely completion of their entries. The accuracy is often verified by checking with both government and commercial sources of data.

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:

Moderate risk attaches to the sensitive information in OCEAN, not only because some of it is SPII, but also because it pertains to investigations about alleged criminal conduct targeting senior EPA officials and implicates reputations of those adversely mentioned. Privacy risk is also associated with the sources of investigative information and could arise from lack of creditability/accuracy of public data and accuracy of data obtained during the investigative process including malicious claims. Leakage of unproven claims can harm an individual's reputation which is a privacy risk that we must address. Privacy risk also exists in case of unauthorized access, sharing or release of information on leads or open cases resulting in harm to witnesses, victims, or investigation subjects.

Mitigation:

Several layers of controls have been deployed on OCEAN to secure sensitive information. These include the agency network security process, Cloud Vendor's network security process, OCEAN roles which control access to PII/SPII for only those with a need to know, and authorized user activity audits. All OCEAN users are required to read and accept the rules of behavior which outlines the risk of unauthorized access. Information about threats to officials sourced from investigative activities, including tips, complaints, interviews, surveillance, records review, evidence collection and analysis, and judicial action is validated, and claims are checked for veracity using appropriate evidentiary standards.

Section 3.0 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.

3.1 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?

There are 9 levels of access, and they are administered by Role. A person's role is tied to their line of work. For example, a Special Agent has different access levels than an Attorney. In addition, assignments to Investigations and certain documents have restrictions for 6e (Grand Jury), Confidential Business Information (CBI), and Confidential Informant (CI) information. In addition, access is restricted by geography through the Organizational Hierarchy. For example, a Supervisor in Region 1 will only have full access to data in Region 1.

The Roles are assigned by the EPA Administrator for OCEAN when the employee's User ID is created. Changes, such as Supervisor to Special Agent or vice versa, as well as geographic/Organizational Hierarchy are adjusted by an EPA Administrator. Assignment to Investigations, and levels, are done either by a Supervisor, or by an EPA Administrator upon request.

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

Determined through roles, depending on job titles and location. These are documented in the system in the Administration, System Roles, section of the application. There are System Permissions, Tracked Data Permissions, and Reference Data Permissions.

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

No.

3.4 Who (internal and external parties) will have access to the

data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

EPA Internal Use Only

Access is granted to OECA/OCEFT/CID Personnel

Contract through Chainbridge to maintain the system. The contract number is GS-35F-0240P. The contract has, or is in the process of being modified to have, the following FAR clauses in it:

FAR 31.205-43

FAR 31.205-46

FAR 52.217-8

FAR 52.217-9

FAR 52.224-1, 52.224-2, 52.224-3;

FAR 52.239-1

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

See EPA Records Schedule 0684 and 1044(e);
https://www.epa.gov/sites/production/files/2018-03/documents/20180309_epa_records_schedules_in_final_status.pdf

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.

3.6 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 the stated purpose and mission of the system.

Privacy Risk:

There are risks of storing data past the retention schedule due to failure to conduct reviews to identify data to be retained or destroyed. Information retained longer than needed could be unintentionally released to or accessed by unauthorized individuals.

Mitigation:

OCEAN users regularly review their cases through weekly and monthly reports, OCEAN users determine record removal when cases or leads are closed or referred to the Department of Justice. OECA also conducts an annual review of the information against the applicable RECORD SCHEDULE 0684.

Section 4.0 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.

4.1 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. Information regarding cases is shared with the DOJ and may be shared with other partner federal access the system, and any information sharing must be initiated by those employees.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

The data in OCEAN involves criminal investigations. Sharing with DOJ is critical for prosecution. Sharing with partner investigative agencies is critical for investigative purposes.

4.3 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?

There are no information sharing agreements because no other organizations within EPA or outside the Agency have access to the system. Access to the system is limited to the EPA Criminal Investigation Division, EPA attorneys, and other administrate staff that support the criminal program.

4.4 Does the agreement place limitations on re-dissemination?

N/A—there are no such agreements.

4.5 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:

Inappropriate or untimely disclosure of information by those who receive it.

Mitigation:

DOJ prosecutors are fully aware of the legal requirements that may affect the disclosure of information and are required to follow the applicable laws. CID controls the disclosure of information to partner agencies and routinely seeks legal counsel to ensure proper information management.

Section 5.0 Auditing and Accountability

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

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

As documented in the OCEAN System Security Plan (SSP for the Monitoring and Auditing (AR) controls, the OECA Program Office utilizes the Risk Management Framework strategy and process to comply with privacy protection requirements and minimize the privacy risk to individuals. OCEAN is subject to annual third-party security assessments conducted by FAA. OCEAN team members perform regular reviews of login auditing to monitor access. OIG conducts monitoring and auditing privacy controls and internal privacy policies on a continuous basis to ensure effective implementation of this procedure. Additionally, the agency Privacy Office conducts annual reviews to evaluate the PII data collected and inquires whether PII data is still required. OECA responds to these annual FIS data calls that are used to determine if the collection of PII is relevant and necessary to accomplish the mission. These data calls assist in ensuring data collected and retained is for the specific documented purpose. In response to the FIS data call, the OECA re-evaluates the information collected and validates the need for that information.

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

This training has been conducted via annual Information Security and Privacy Awareness Training, The OCEAN system administrator and system owner also attends annual required role-based training provided by EPA.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a risk of unauthorized access, modification, deletion and/or release of sensitive data. If an agent leaves or transfers to another office and their OCEAN account is not deactivated, there is a risk that agent may still access OCEAN and related PII/SPII. Unauthorized release of audit and event logs could expose agent activity and physical location through IP address.

Mitigation:

Consistent training to ensure awareness. Also, case-specific information management guidelines are provided by knowledgeable EPA attorneys/DOJ prosecutors. Ensuring accounts are deactivated for users that no longer need access to OCEAN, Regular review of event/audit logs, and ensuring only system administrators have access to even/audit logs.

Section 6.0 Uses of the Information

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

6.1 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. See 40 CFR 16.11 and 16.12. 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.

To gather leads from open-source intelligence (including from the internet, public records, recordings, and letters) on threats to the EPA Administrator, other senior executive service mangers, or their family members.

6.2 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.

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

The previous system of records for the information was the EPA System of Records EPA-17, Criminal Investigative Index and File (also known as Criminal Case Reporting System (CCRS)), for which a Federal Register Notice was last issued at 71 FR 342 (Jan. 4, 2006). A modification SORN for EPA-17 was issued, declaring the software modernization, expanded content, and new name for EPA-17: the Online Criminal Enforcement Activities Network. It was issued on 08/02/2019. The URL is: **https://www.federalregister.gov/documents/2019/08/02/2019-16565/privacy-act-of-1974-system-of-records**

6.4 Privacy Impact Analysis: 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.

Privacy Risk:

Although the system is exempt from Privacy Act Request procedure, discretion that is permitted to allow amendment, sharing, inspection or acquisition of copies of the record might be exercised wrongly, resulting in privacy harms to individuals (e.g., witnesses).

Mitigation:

Several layers of controls are deployed on OCEAN to ensure information is used for specified purposes only. Records management procedures, including security clearances, training, and code of conduct apply. This includes PL-4 – Rules of Behaviors, CIO 2151.1 - Privacy Policy, and CIO 2150-P-21.0 – Information Security – National Rules of Behavior. Access controls ensure access by specified users only. OECA employees read, understand, and accept the rules of behavior. If they decline, they will not have access to OECA network or systems. OCEAN users also take annual security training and for those with privileged access, at least two role-based security training per

year. Regular users sign off on the rules of behavior while those with Privileged access, complete the Privileged User RoB.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 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.

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

No prior notice is provided, because the data involves ongoing criminal investigations; or involves EPA discovery, receipt, or searches of open-source online information, or other information or records outside the agency. In short, the records are exempt from Privacy Act notice. See 40 CFR 16.11 and 16.12. Pursuant to 5 U.S.C. 552a(j)(2), this system is exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f)(2) through (5); and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in that subsection: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f)(2) through (5). See, 40 CFR 16.11 and 16.12.

7.2 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?

Individuals do not have the opportunity to decline or provide information, or to opt out of the collection or sharing of their information.

7.3 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:

Privacy risk arising from notice requirements is minimal. The Privacy Act of 1974 affords

individuals a right to notice in order to provide consent or become aware of data actions involving their information. However, there are exceptions to this requirement pursuant to 5 U.S.C. 552a(j)(2).

Mitigation:

Judicious exercise of discretion to provide notice on a case-by-case basis, taking into consideration Privacy Act exemptions that apply and protection of interests involved including integrity of investigations and the safety of witnesses and investigative subjects.

Section 8.0 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.

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

None. Pursuant to 5 U.S.C. 552a(j)(2), this system is exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f)(2) through (5); and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in that subsection: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f)(2) through (5). See, 40 CFR 16.11 and 16.12.

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

None**.** Pursuant to 5 U.S.C. 552a(j)(2), this system is exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f)(2) through (5); and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in that subsection: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f)(2) through (5). See, 40 CFR 16.11 and 16.12.

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

None**.** Pursuant to 5 U.S.C. 552a(j)(2), this system is exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f)(2) through (5); and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in that subsection: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f)(2) through (5). See, 40 CFR 16.11 and 16.12.

8.4 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:

There is no privacy risk as, pursuant to 5 U.S.C. 552a(j)(2), this system is exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f)(2) through (5); and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in that subsection: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f)(2) through (5). See, 40 CFR 16.11 and 16.12.

Mitigation:

As there is minimal to no risk.