EPA United States
Environmental Protection
Agency

PRIVACY IMPACT ASSESSMENT
(Rev. 04/2019)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, send a request to: privacy@epa.gov.

System Name: National Case Status Information System (NCIS)

Preparer: Cindy Hobus	**Office:** Office of Enforcement and Compliance Assurance
Date: 01/23/2020	**Phone:** 202-564-8143

Reason for Submittal: New PIA__X   Revised PIA____   Annual Review____   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:

The National Case Status Information System (NCSIS) OECA Docket is an internal tool developed to allow the Office of Enforcement and Compliance Assurance (OECA) Assistant Administrator's (AA) office to review in progress enforcement and compliance cases being handled by the Office of Civil Enforcement (OCE), Federal Facilities Enforcement Office (FFEO), and Regional Offices at any given moment. This case management system relies on a central case status system to share case data between OECA and the Regions. The tool provides an automated means to enter the specific case data into a repository via an upload that is accessible by the OECA AA's office. The NCSIS OECA Docket does not generate new data.

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?

OECA works with EPA regional offices, and in partnership with state and tribal governments, and other federal agencies to enforce the nation's environmental laws, including:

- Clean Air Act (CAA 42 U.S.C. §7401 et seq.)
- Clean Water Act (CWA 33 U.S. Code § 1251 et seq.)
- Comprehensive Environmental Response, Compensation and Liability Act (CERCLA, or Superfund 42 U.S.C. § 9601 et seq)
- Emergency Planning and Community Right-to-Know Act (EPCRA 42 U.S.C. §11001–11050)
- Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA 7 U.S.C. §136 et seq)
- Marine Protection, Research and Sanctuaries Act (MPRSA 16 USC § 1431 et seq. and 33 USC §1401 et seq.)
- National Environmental Policy Act (NEPA 42 U.S.C. § 4321 et seq.)
- Oil Pollution Act (OPA 33 U.S.C. 2701 et seq.)
- Resource Conservation and Recovery Act (RCRA 42 U.S.C. §6901 et seq.)
- Safe Drinking Water Act (SDWA 42 U.S.C. §300f et seq.)
- Toxic Substances Control Act (TSCA 15 U.S.C. 2601 et seq.)

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 NCSIS system security plan is being prepared now in Xacta. The system ATO is in process and is expected to be issued sometime in early June 2020 as it is pending a FAA Assessment scheduled for May 18, 2020.

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?

No.

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).

NCSIS collects, uses, disseminates and maintains the following information:

	Field	Definition and/or Instructions for Entering Data Elements
1	NCSIS Case ID	Unique identifier.
2	Region/HQ Office	The Region or HQ Office entering the data.
3	Statute	Primary law and section selected from a predefined set of primary laws and sections.
4	Company / Case Name	The case name used in ICIS, or, if the case is not in ICIS, the name of the facility/site. If there happens to be independent active cases involving the same facility, the company/case name in each NCSIS record must be different to distinguish between the two cases.
5	FRS ID Number or Lat/Long when no ID available	Facility Registry System (FRS) identification number. When entering lat/long insert decimals separated by a comma (e.g., 38.5998, -90.0000).
6	Address	Facility/site street address. For multi-facility cases, the address entered should be the corporate address.
7	State	State where the facility/site is located. For multi-facility cases, the state entered should be the state listed in the corporate address.
8	Authorized Program / EPA has Direct Implementation	Where EPA's authorities provide, and where states or tribes are eligible, willing, and able, and apply to EPA for such authority, EPA may approve states or tribes to assume regulatory and program management responsibilities in states or Indian country. However, until state or tribal governments are willing and able to assume full responsibility for delegable programs, EPA generally retains responsibility for managing federal environmental programs in states or Indian country. This responsibility of the EPA is known as direct implementation.
9	State Onboard	The possible positions that a State might take with regard to a case.

	Field	Definition and/or Instructions for Entering Data Elements
10	Violation(s)	Briefly (1 or 2 sentences) set forth the facts that, in combination with the law and evidence discussed, comprise the violation(s). More specifically, describe the facts of the violations and the environmental consequences, as well as any other information relevant to the seriousness of the violations. When changes are made to this field the date the change is made should be inserted.
11	Key Considerations (Procedural Posture of Case/Enforcement Action Type(s) and Important Milestones/Steps)	All interim Enforcement Action Types and important milestones/steps in the case such as: status of negotiations (e.g., referral sent to DOJ; negotiation kick-off letter sent to respondent, 1st settlement meeting held, counter-offer presented to respondent, agreement in principle on injunctive relief and penalty reached, complaint drafted, received SEP proposal from respondent, tolling agreement in place through XZY date; consent decree lodged); status of litigation (e.g., a discovery deadline is pending, a summary judgment motion has been filed, preparing for a deposition, prepping expert witness, a proof of claim has been filed by DOJ, an oral argument is scheduled, a brief is being prepared); and any other sensitive or significant issues (e.g., ISE orders, press or congressional interest, precedential issues). Identify the date an Enforcement Action Type and important milestone/step is completed (do not delete).
12	Planned Enforcement Action	The enforcement action type. See the Enforcement Action Type table below for a list of enforcement action types. The Enforcement Action Type selected should be kept up to date and reflect the latest interim stage of the case.
13	Action Planned Date	The date when the planned enforcement action is expected to be issued.
14	Inspection Date	The first day of the inspection.
15	Action Actual Date	The date the planned enforcement action is issued.
16	National Compliance Initiative	Cases taken under one of EPA's national compliance initiatives.
17	Nationally Significant Issue	Cases that include a nationally significant issue pursuant to applicable guidance.
18	Proposed Penalty Value	Proposed or assessed penalty value. Can change as case develops.
19	Regional / OCE Division Manager	Appropriate manager in the Region or HQ Office.
20	HQ Interest	Cases of particular interest to HQ.

Additionally, NCSIS uses the following information to allow access to the application; track changes made to the data by users of the application; and to save preferred settings of fields visibility for the

table view in the application interface. This information is stored in a table in the database and not available to users on the front end. The table field names and definitions are:

	Field	Definition and/or Instructions for Entering Data Elements
1	userid	Web Application Management (WAM) user id created via NCC Web Application Access user management service.
2	username	User's first and last name
3	fields	A JSON array of fields and values to customize the user's displayed table in the web application
4	role	admin, editor, or reviewer. Admin is the same as editor since no other features are available to admins. Reviewers have read-only access.

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

Enforcement and compliance case status information sources originate in the Regional Offices, OCE, and FFEO and shared among the Regional Offices, OCE, FFEO, and the Enforcement Targeting and Data Division in the Office of Compliance. The information is used by OECA senior enforcement managers to track progress of cases meeting the specified selection criteria. Information is entered or uploaded via a spreadsheet into the system by authorized internal EPA users only. All NCSIS internal users use the single sign-on (SSO) LAN ID and password to access the system. The system does not accept or store any confidential business information.

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.

The national case system design team has created a series of data categorization lists that can be used as data entry drop-down lists to help ensure that everyone is using the same terminology for captured data elements, optionally using the specific internal codes for each item in a drop-down list. The system does not provide extensive data validation, but instead relies on the staff providing accurate data entry. Statuses are reviewed and updated as needed on a monthly basis.

2.5   <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>:

There is a privacy risk for users of the application as personally identifiable information is available to NCSIS administrators and could be expose. There is also a risk for EPA staff who are listed as POCs in the application for enforcement cases as their name is available to all users of the application and the application maybe compromised.

<u>Mitigation</u>:

Access to the NCSIS system is limited to authorized internal users only (i.e., only EPA HQ and regional staff with justification for access to NCSIS and EPA direct contractors authorized to maintain the application). There are privacy controls in place that do not allow external users to access NCSIS. Users will need to use their EPA authorized LAN ID and password to access NCSIS.

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?

Yes. WAM is used to authenticate all authorized internal users to access NCSIS. Authorized users are Regional, OCE, and FFEO points of contact (POCs) that upload data to NCSIS as well as POCs in the AA's Office that review this information. No external users have access to NCSIS. Editor and Read Only roles are assigned to users to control which users have access to add and edit case data.

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

Only designated staff with case knowledge in the Regional Offices, Office of Civil Enforcement, and the Enforcement Targeting and Data Division in the Office of Compliance (OC) gain access to NCSIS through the WAM portal. Authorized staff in the OC Headquarters office grant user access to the application. Users are required to log in to the application with their LAN ID and password or PIV card. First time users get added to the users database table. The table includes a user name, LAN

ID, and role of the affiliated user. More information regarding access controls is provided in the NCSIS Role Based Access document saved as an artifact in the NCSIS project in Xacta.

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?

- Internal users include: US EPA staff in the Office of Civil Enforcement, and the Enforcement Targeting and Data Division in the Office of Compliance, and EPA Regions 1 through 10.
- Contractors to US EPA staff in charge of system administration and the ERG contract supporting the NCSIS system. Appropriate FAR clauses are included.
- No external users have access to NCSIS.

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.

Records schedule 1044(a) applies. Enforcement records maintained by the Office of Enforcement and Compliance Assurance (OECA) and related to enforcement of EPA statutes, regulations and standards, including case development and litigation support files, background studies and surveillance reports, legal opinions, attorney work products, violation notices, press releases, compliance orders, and related records. There is no time limit on how long each record is retained. Currently the system is designed to store the data indefinitely.

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:

The privacy risk associated with degeneration of data, deletion or loss of data or huge data storage over time is low because it is a duplication of case information maintained by the Regional and Headquarters case managers.

Mitigation:

Instead of being a warehouse of enforcement cases, only a subset of active enforcement cases cases of interest are added to the NCSIS.. EPA records schedule 1044(c) applies to case data containing

7

EPA case manager point of contact information. These records are disposable and are destroyed 20 years after file closure. Application user information is removed when a user no longer requires access to the system.

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.

No.

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

Not applicable.

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?

Not applicable.

4.4   Does the agreement place limitations on re-dissemination?

Not applicable.

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:

None, no information is shared externally.

Mitigation:

None.

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?

Every user must acknowledge that they are accessing an EPA data system and use it properly.

Example: Pre-Sign-In Notification language for all EPA staff and EPA contractors that access the system:

In proceeding and accessing U.S. Government information and information systems, you acknowledge that you fully understand and consent to all of the following:

1) you are accessing U.S. Government information and information systems that are provided for official U.S. Government purposes only

2) unauthorized access to or unauthorized use of U.S. Government information or information systems is subject to criminal, civil, administrative, or other lawful action

3) the term U.S. Government information system includes systems operated on behalf of the U.S. Government

4) you have no reasonable expectation of privacy regarding any communications or information used, transmitted, or stored on U.S. Government information systems

5) at any time, the U.S. Government may for any lawful government purpose, without notice, monitor, intercept, search, and seize any authorized or unauthorized communication to or from U.S. Government information systems or information used or stored on U.S. Government information systems

6) at any time, the U.S. Government may for any lawful government purpose, search and seize any authorized or unauthorized device, to include non-U.S. Government owned devices, that stores U.S. Government information

7) any communications or information used, transmitted, or stored on U.S. Government information systems may be used or disclosed for any lawful government purpose, including but not limited to, administrative purposes, penetration testing, communication security monitoring, personnel misconduct measures, law enforcement, and counterintelligence inquiries

8) you may not process, or store classified national security information on this computer system and

9) By using your PIV card to electronically sign Agency documents, you acknowledge that

you have the same intent as would be required for an authorized handwritten signature to any Agency documents.

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

All EPA users are required to participate in Security and Privacy Awareness Training annually.

5.3 <u>Privacy Impact Analysis</u>: Related to Auditing and Accountability

<u>Privacy Risk</u>:

The privacy risk is low associated with improper access to NCSIS as well as incorrect auditing and use of NCSIS information relative to the technical and policy-based safeguards and security measures in place.

<u>Mitigation:</u>

Access to NCSIS is restricted to the EPA internal network only. All users accessing NCSIS must first acknowledge and consent to the proper use of the EPA's data system and participate in EPA's annual Security and Privacy Awareness training. NCSIS relies upon the hosting environment for auditing events outside of the purview of NCSIS, including system and application logs. Regarding information in the NCSIS application, as part of routine maintenance, data changes are reviewed.

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 OECA senior enforcement managers are expected to have full situational awareness of all nationally important enforcement and compliance cases being handled by the EPA headquarters (HQ) Offices (OCE and FFEO) and Regional Offices at any given moment. Existing tools were deemed unsatisfactory to accomplish this goal. So, in Q2-FY18, OECA's AA and DAA requested the Data, Innovations & System Council (DISC) to investigate the creation of a software tool that can be used to share case information that already exists in regional and HQ Office systems with a dynamic query system suitable for use by the AA and DAA. That NCSIS has been developed in a cooperative effort between the Regional Offices, Office of Civil Enforcement, and the Enforcement Targeting and Data Division in the Office of Compliance to connect Regions and HQ Offices to a national data system.

6.2   How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_   No_X_. 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.)*

A user can save their view settings related to data table column visibility in the user interface. A user's saved settings are retrieved using the user's EPA LAN id when they log into the application via WAM. This is a validation process only.

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

None.

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:

The risk related to improper use of information is low. The risk is that a NCSIS user that is the owner of a case record may edit a record incorrectly.

Mitigation:

Internal user agreement for accessing EPA data systems is required before accessing the system. NCSIS system controls included role-based editing access versus reviewer role for read only access. In addition, there are data categorization lists for the data collected that are used as data entry drop-down lists to help ensure consistent captured data elements.

*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.

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?

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:

Mitigation:

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?

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

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

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:

Mitigation: