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: System Name: Superfund Cost Recovery and Imaging Online System (SCORPIOS)	
Preparer: Andrew Lam	**Office: OCFO/OTS/IMSD**
Date: 4/27/2018	**Phone: 202-564-2925**
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: 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:

SCORPIOS is used to organize cost information and produce reports that summarize the costs for a specific Superfund Response, Brownfield Program, or Oil Spill site. Additionally, Federal Emergency Management Agency (FEMA) mission assignment costs can be tracked if a specific incident is assigned a site/project identifier or a mission assignment Organization Code. Together the cost report and the supporting cost, and technical documentation will yield a Cost Documentation Package.

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?

The SORN (EPA-39) documents the system's legal authority to collect, maintain and use privacy information. Comprehensive Environmental Response, Compensation, and Liability Act of 1980, 42 U.S.C.9607; 5 U.S.C. 301; 31 U.S.C. 3512; Executive Order 9397 (Nov. 22, 1943).

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.

No ICR required.

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).

Financial data and associated documents (images) are collected, major grouping includes travel, payroll, and voucher data.

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

The source of information comes from the Compass Data Warehouse (CDW). CDW is a repository of Compass data and its predecessor system. The types of information are financial data and associated document pdf images, travel, payroll and voucher data for cost recovery efforts.

PII exists in two forms within Scorpios.

The first form is that the SSN is data base key for Employee Masterfile. Due to the SF record retention requirement of 30 years, we are required to maintain Payroll Data and related PDF timesheets for almost of the Superfund Sites to which employees charged

time. EPA did not deploy the Employee ID (EMPID) process until the implementation of People Plus in FY 2005.

The risk of an authorized Scorpios User accessing SSN system data will be mitigated via Scorpios Modernization replacement application (expected release 6/2019) will remove all SSN data in Scorpios and replacement with actual or retroactively assigned EmpIDs. The secondary form of PII in Scorpios is usually found on pre-People Plus timesheets and pre-Travel Manager invoices and related receipts.

CDW collects other Non-PII data from other agency systems such as the Contract Payment System, IDOTS, GPAS/IGMS, EAS and Contract Laboratory Sample cost tracking systems.

Other than scanning the early timesheets and travel invoices directly into Scorpios all PII data is collected in EPAs Payroll and Electronic Travel systems.

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.

SCORPIOS relies on internal control in Compass and CDW to ensure accuracy 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:.

Individuals who participate in cost-recoverable superfund cleanup activities are to have their labor data such as employee number, time, location, and duration of superfund work collected into the SCORPIOS database.

Mitigation.

Privacy is protected by physical controls as well as by logical access controls that protect the data stored in the database. The national computing center physical facility has extensive physical controls such as guards, gates, locks, and other access controls; the logical access controls to the database include requirements for identification and authentication, audit

controls, data integrity protection, and data transmission protections

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.

Cost data (and supporting documentation) is integral to cost recovery efforts and required by the federal rules of evidence in litigation. Without detailed cost information (reports & documents) EPA would not be able to recover its cleanup costs from responsible parties. All of this data is essential to the Agency's accurate and timely performance of its cost recovery efforts.

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.)

SSN, Name.

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

The type/elements of information about the user are being retrieved in SCORPIOS such things as social security number, name, other personal identification numbers, personal information related travel expenses such as home addresses, credit cards, and other recoverable expense items.

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

SORN # 39

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.

The system does not use technology to conduct electronic searches, queries, or analyses in

an electronic database t discover or locate a predictive pattern or an anomaly.

3.6 Privacy Impact Analysis: Related to the Uses of Information

When we need to release PII data. That information is redacted. Prior to the electronic payroll and travel systems, many regions redacted PII concurrently as the documents were scanned into Scorpios. Since regional Superfund accountants are no longer part of the process of importing travel receipts into Scorpios, most regions require the travel receipts to be redacted as soon as the Superfund site comes up for an internal review. Where DOJ indicates that they may be releasing PII on documents to Potentially Responsible Parties, all regions should have redacted PII before sending a final releasable cost package to DOJ. er.

There is no risk by sharing externally, Users level risk could be there if a SCORPIOS user does not maintain proper control. Control over PII.

Privacy Risk:

Risk of SCORPIOS users that have access to the data inadvertently not follow EPA procedures in handling PII.

Mitigation:

Limit access to users based upon need. All external reporting that have PII are removed. All PII is redacted before allowing DOJ and/or Coast Guard to release documents outside of their agency.

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.

The 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 Agency Privacy Officer.

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?

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.

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:

None.

Mitigation:

None

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?

Yes, The SCORPIOS system incorporates group-based access controls that limit the users' rights by what information they need to review or activities they need to perform. The user's role is identified by the employee's supervisor, and approved by regional/national system administrators and then the SCORPIOS system Security Administrator.

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

Refer to 5.1

No.

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)?

We do not allow the public or outside parties to access the system. Only authorized users (EPA personnel, SEE employees and EPA contractors) that have had a proper background check can have access to the system. FAR clauses are incorporated into the applicable EPA contract. Prospective users must complete an appropriate OPM Investigations i.e. (Low Risk Level-NACI; Moderate-MBI; Moderate for IT position-LBI; High-BI) prior to hiring and being granted access to SCORPIOS.

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

The SCORPIOS system is accessed by only authorized users (EPA personnel, SEE employees and EPA contractors) who work with Superfund cost recovery data that have had a proper background check can have access to the system. Prospective users must complete an appropriate OPM Investigations i.e. (Low Risk Level-NACI; Moderate-MBI; Moderate for IT position-LBI; High-BI) prior to hiring and being granted access to SCORPIOS.

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.

Superfund cost recovery records are retained for at least 30 years after the completion of all cost recovery at a given Superfund Site.

014/a1 SFD Remedial Site-specific files (FSD) / 30 year permanent (transferred to NARA).
024 Cost Recovery (contract specific)/30 year temporary (destroyed)

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

N/A

Yes. 014/a SFD Remedial Site specific files (SFD0 / 30 year permanent (transferred to NARA).

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:

Trying to determine what superfund sites stopped cost recovery efforts before 1988 is

problematic. We have to follow the retention requirement. We just had a Superfund site in active litigation that included costs and supporting document back in 1986

Mitigation:

N/A

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.

There are 3 categories regarding information sharing for SCORPIOS: Coast Guard, DOJ, and the Potential Responsible Party (PRP). DOJ and Coast Guard have MOUs. There are 2 Agreement types for PRP: Protective Order Agreement – court order signed by a judge to protect EPA information; Confidentiality Agreement (Agreement between EPA lawyer and other party lawyer). We share financial and cost data but not PII.

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.

Agreement/compliance regarding to PII data. EPA does not share PII data externally.

6.3 Does the agreement place limitations on re-dissemination?

Yes.

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

This may be a new feature for the new replacement SCORPIOS.

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?

SCORPIOS does not review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organization within EPA and outside. Most regions track when costs package is compiled by finance offices and when they are shared to Legal and Enforcement Staff. The Finance SCORPIOS users are not usually part of the decision process of whether or to whom a package will be realeased.

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:

Information provide to Coast Guard may include (unredacted) PII on travel receipts. PII information shared with US Coast Guard is pursuant to a MOU that details how USCG Will protect PII and CBI.

Mitigation:

Information provide to DOJ is redact with PII.

Where DOJ might release PII and/or CBI, protective order or confidentiality agreement are in place.

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?

Users only have read access, they can only see their PII data, they can't correct their data. Individuals who want to access to their records should make a written request to the Agency Privacy Officer..

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

None.

Individual who wants to contest the content of a record should make a written request to the Agency Privacy Officer.

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

The system does not notify individuals about the procedures for correcting their information. Any individual who wants to contest the contents of a record, should make a written request to the Agency Privacy Officer.

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:

N/A

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?

The SCORPIOS system incorporates group-based access controls that limit the users' rights by what information they need to review or activities they need to perform. The user's role is identified by the employee's supervisor, and approved by regional/national system administrators and then the SCORPIOS system Security Administrator.

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

The system administrator provides privacy training to the users. Additionally, users are required to take the Annual IT Security Awareness training in order to obtain access to EPA systems.

8.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Unauthorized users access the system to see PII data.

Mitigation:

The SCORPIOS system incorporates group-based access controls that limit the users' rights by what information they need to review or activities they need to perform. The user's role is identified by the employee's supervisor, and approved by regional/national system administrators and then the SCORPIOS system Security Administrator.