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: Compass	**System Owner: Michael Clanton**
Preparer: Andrew Lam	**Office: OCFO/OTS/IMSD**
Date: 2/9/23	**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: 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:

Compass Financials is an EPA major information system. Compass Financials was developed in October 2008 and is currently in the operations and maintenance phase. Compass Financials is a web application developed by CGI Federal Incorporated using object-oriented design methodologies and development techniques. It provides the tools needed to effectively manage, budget and track expenditures. Compass Financials supports the financial management information requirements of both managers and administrative staff. It provides financial information at both detailed and summary levels in a variety of formats, which enables agencies to evaluate and analyze the cost of operations.

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?

Compass. 31 U.S.C. 3701(a)(30) and 15 U.S.C. 1681a(f).

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?

Yes. A system security plan has been completed for the information system supporting the system. The system has an Authorization-to-Operate. The ATO expires on 10/26/2025.

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 Information Clearance Request is required. And no OMB forms are created for Compass.

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?

The data will be maintained or stored in the cloud. The Cloud Service Provider (CSP) is FedRamp approved. CSP provides infrastructure as a service (IaaS), Software as a service (SaaS) for EPA.

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, Financial Information (accounts receivable including interest calculations, dunning functions, and cash receipts); accounts payable (including interest, handling and

penalty calculations and making automated disbursements); and travel obligations, issue advances, and pay both the traveler and third-party vendors.), Social Security Number (SSN), Telephone Number, Bank Routing and Account Number.

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

The sources are other IT systems. Compass itself does not collect this information directly. Information is gathered indirectly from feeder systems and transmitted via internal and external batch jobs which run nightly, and in real time, depending on the information system. Compass currently has 17 connections with internal and external parties.

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

Does not use information from commercial sources.

2.4 Discuss how accuracy of the data is ensured.

All information goes through a two-step process in the feeder systems and then is verified again in Compass.

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:

Compass servers could be hacked and data could be manipulated.

Mitigation:

To alleviate the privacy risk, Compass uses the following security safeguards: server encryption, network firewalls, and multi-factor user access to ensure accurate data is being input into the system.

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, select authorized users are granted the creator role or the approver role, but they are required to have a waiver that is signed by the Office of the Comptroller.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

The Compass Standard Operating Procedures for granting access.

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

The roles and responsibilities are assigned to EPA Office of Toxic Substance (OTS) employees or contractors.

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 employees and OTS contractors. The FAR clauses are in their contracts.

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 are maintained for 6 years and 3 months after final payment. They are deleted when no longer needed, unless related to the Superfund program cost recovery efforts. Superfund cost recovery records are maintained more than 30 years after the completion of cost recovery at the site. The Records Control Schedule is #54.

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 data stored in Compass are kept active in the system for too long.

Mitigation:

To alleviate the risk of over retention in Compass, records are maintained up to 6 years and 3 months after final payment and then deleted. During this time, hard copies of transactions are stored in a secured room only limited to personnel who has a need to know. Those hard copies are destroyed at a certain set time as well.

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.

To the Office of Management and Budget and the Department of Treasury for the Purpose of carrying out the EPA's financial management responsibilities. Another use for Treasury is to identify and prevent payment errors, fraud, and abuse within federal spending. To provide debtor information to debt collection agencies, under contract to the EPA, to help collect debts owed to EPA. Debt collection agencies will be required to comply with the Privacy Act and their agents will be made subject to the criminal penalty provisions of the Act.

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

To the Office of Management and Budget and the Department of Treasury for the Purpose of carrying out the EPA's financial management responsibilities. Another use for Treasury is to identify and prevent payment errors, fraud, and abuse within federal spending. To provide debtor information to debt collection agencies, under contract to the EPA, to help collect debts owed to EPA. Debt collection agencies will be required to comply with the Privacy Act and their agents will be made subject to the criminal penalty provisions of the Act.

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?

We follow the standard process of getting Memorandum of Understanding (MOU)/Information Sharing Agreements (ISA) approved through the management chain, to include the Chief Information Officer (CIO) approval.

4.4 Does the agreement place limitations on re-dissemination?

Yes. Use of data is covered in the MOU/ISA between interconnecting systems.

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:

Information shared with Treasury/OMB may be compromised if handled inappropriately.

Mitigation:

MOU/ISA between EPA and U.S Treasury/OMB describes the PII within the information system and the purposes for its distribution and how the data should be protected. To mitigate the risk of information being shared inappropriately, EPA users must take the privacy awareness training to ensure that they understand EPA privacy responsibilities and procedures.

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 as stated in Section 6.1?

There is a standard operating procedure (SOP) that has been developed to enforce the sole use and purpose of collection. Individuals that have access to this system agree to use the system strictly for the purpose of collection.

All users are subject to security controls and roles in the system. They all have at least a basic North American Industry Classification System (NACIS) background screening. All EPA personnel with access to sensitive data are required to undergo a higher l level of background screening sponsored by EPA. All passwords automatically expire after 30 days of non-use.

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

EPA personnel and contractors are required to complete an Information Security and Privacy Awareness and Training course on an annual basis. The training course instructs personnel to not disseminate PII information to unauthorized individuals and how to secure information using approved techniques such as encryption.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Unauthorized user accessing the system or an user who tries to access any data in Compass.

Mitigation:

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

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.

This system is the EPA's System of Records for financial data and contains information on EPA travel, accounts payable and accounts receivable, budgeting and funds management activities. It provides the tools needed to effectively manage, budget and track expenditures.

Compass Financials supports the financial management information requirements of both managers and administrative staff. It provides financial information at both detailed and summary levels in a variety of formats, which enables agencies to evaluate and analyze the cost of operations. All Compass Financials subsystems are fully integrated, so that transactions update budgets, financial plans, and the general ledger at the time they are processed. Compass Financials provides local users with the flexibility to establish and maintain operating plans and provides users in the EPA with the information needed for consolidated financial reporting and control. It provides debtor information to debt collection agencies, under contract to the EPA, to help collect debts owed the EPA. Debt collection agencies will be required to comply with the Privacy Act and their agents will be made subject to the criminal penalty provisions of the Act.

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.*)

User Id

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

None. Compass is a financial system, and it receives PII data from People Plus (PPL) and

Payment Tracking System (PTS). Data sent from PPL and PTS to Compass is encrypted, there are network firewalls in place, multi-factor authentication is used for user access, role-based access and security background checks of individuals who have system access to the PII are performed.

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:

Users mishandle Compass PII.

Mitigation:

To reduce the likelihood of mishandling of PII in Compass, Privacy Awareness Training is provided to ensure that personnel understand privacy responsibilities and procedures. EPA personnel and contractors are required to complete an Information Security Awareness and Training course on an annual basis. The training course instructs personnel to not disseminate PII to unauthorized individuals, how to secure information using approved techniques such as encryption, and proper destruction and disposal of PII. Individuals who have system access must have a security background check. Compass only grants access to users based on the principle of least privilege which provides user sufficient access to perform their jobs, no higher than necessary to accomplish their organizational missions/business functions.

***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 it doesn't. However, any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Requests must be submitted to the Agency contact indicated on the initial document for which the related contested record was submitted. Complete EPA Privacy Act procedures are set out in 40 C.F.R. part 16.

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:

No risk because the notice for collection of information was publicized according to EPA policy.

Mitigation:

There is a notification procedure outline in SORN EPA-29

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?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card) and follow guidance described in section 7.1 of this PIA. Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 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 described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 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:

Individuals' records could be provided to the incorrect requestor.

Mitigation:

EPA's Privacy Act request process ensures the requestor give appropriate identification during a Privacy Act and/or FOIA Request before EPA can share any records that EPA may maintain on that individual.