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: eBusiness	
Preparer: William Lominack (Owner) Olamide Akinbobola (ISSO)	**Office:** OMS/OITO/SBMD
Date: 02/02/2022	**Phone:** 919-541-5461
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:

eBusiness is an EPA web-based application available via the EPA intranet that provides the functions to support the Working Capital Fund (WCF). eBusiness is where Agency-wide users establish the necessary accounts needed to order and manage WCF products and services via the online catalog. The application is role based and requires that users authenticate when accessing the application. This is a catalog for ordering EPA WCF services. As a Service Account manager (authenticated role-based user) you can manage your WCF service agreements, orders, and accounts via eBusiness.

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?

- Federal Information Security Modernization Act of 2014 (Pub. L. 113-283);
- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," revised, July 26, 2016;
- DHS Management Directive MD 140-01, "Information Technology Systems Security," July 31, 2007;
- National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, "Minimum Security Requirements for Federal Information and Information Systems," August 2013; and
- Homeland Security Presidential Directive 12 (HSPD-12), "LincPass", August 12, 2004

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?

eBusiness has an approved ATO, expires June 6, 2022

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. The provisions of the Paperwork Reduction Act are not applicable to eBusiness because information from members of the public is not collected. Only information from EPA personnel, Inside Affiliates, and External Affiliates (partners) is collected.

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, all eBusiness data is maintained and stored at the NCC.

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).

eBusiness connects to other agency authoritative sources (OASIS and Compass) to pull information on EPA employees and other affiliates (Contractors, SEEs, grantees, etc.) for authentication and authorization to agency resources. eBusiness collects this information in order to deliver Working Capital Fund Services (WCF) to Agency customers (employees and affiliates) and not for public users or access. eBusiness is where Agency-wide users establish the necessary accounts needed to shop, order/cancel, monitor, and manage WCF products and services via an on-line catalog. eBusiness provides the means for WCF Activity Managers and Service/Product Managers to accurately provide and charge-back for WCF products and services. eBusiness uses automated registrations, usage submissions, billing, and various reporting features to deliver, manage, and charge for WCF ordered activities across the WCF portfolio.

OASIS PSS Record Number (PID)

2. First Name

3. Middle Initial

4. Last Name

5. ECI / Workforce ID

6. Personnel Type ID

7. Personnel Type Affiliation (Employee or Contractor/Grantee/SEE)

8. Organization Code

9. Organization Description

10. Status (active or terminated)

11. Position Title

12. Date Created

13. Date Modified

14. Location City

15. Location State

16. EPASS Eligible

17. PUC Eligible

18. Security Requirements Met

19. OK to Onboard Indicator

20. Highest BI Value

21. Work Begin Date

22. Hiring Manager Name

23. Hiring Manager Email

24. Hiring Manager Phone

25. Hiring Manager PID

26. Date Created

27. Contract Start Date

28. Contract Expiration Date

29. Contract Number

30. Company Name

31. COR PID

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

Individuals registering for eBusiness application access. (Account Managers)

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.

Data accuracy is responsibility of the system that collects and stores that information. eBusiness simply pulls data from the authoritative source to use in managing the service agreements and orders.

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:

eBusiness is only available to authorized users within the secure EPA network. It is not accessible by members of the public. Users must read, acknowledge, and adhere to the eBusiness rules of behavior. The acknowledgement is recertified annually.

Mitigation:

EPA employees and Internal affiliates are required to take Privacy and Information Security Awareness training annually. Additionally, the eBusiness Rules of Behavior must be read and acknowledged annually.

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. eBusiness offers a number of measures to secure access to data, such access control rules and password authentication. Non-authorized users are prevented from gaining access to eBusiness and mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information. The system uses the Agency's PIV for 2-factor Authentication and role-Based access controls. Least privilege is used for authorized users based on their job roles and responsibilities.

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

eBusiness is a role-based access application. Logical access controls are employed to permit only authorized access to the system and restrict users to authorized transactions, functions, and data. These automated controls ensure that only authorized individuals gain access to information system resources, that these individuals are assigned an appropriate level of privilege, and that they are individually accountable for their actions. These controls support the separation of duties principle.

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

The system protects confidentiality and integrity of data through a number of controls, including restricting read-only or read-write access to data to those authorized users whose roles permit such actions.

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?

eBusiness contractors are required to sign a Contractor Computer User Agreement upon hire which outlines the Rules of Behavior, Acceptable Use, Conflict-of-Interest, and Nondisclosure policies in the use of EPA equipment and resources. Additionally, the FAR clauses 24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act are included in the contract.

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.

The information is retained for the life of eBusiness. The information cannot be purged and is used for financial audit purposes. eBusiness must maintain historical records to accurately document, provide and charge-back for WCF products and services. eBusiness uses automated registrations, usage submissions, billing, and various reporting features to deliver, manage, and charge for WCF ordered activities across the WCF portfolio.

The system follows EPA Records Schedule 0089 Information Tracking System and 1012 Information and Technology Management. Data will be eliminated according to EPA policy for record retention as documented in EPA Records Schedule 704 Personnel Security Case files.

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 no risks associated with having the information needed for retaining the data integrity of eBusiness.

Mitigation:

N/A

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.

N/A

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?

No organizations outside the EPA have access to eBusiness. All the system components for eBusiness are hosted at the NCC in RTP, NC on the internal EPA Network. eBusiness is only accessible to authorized users.
Access within the Agency is determined on a case by case basis. MOU and ISA are created and agreed to prior to any access granted. MOU/ISA in place with OASIS

4.4 Does the agreement place limitations on re-dissemination?

N/A

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

Mitigation:

N/A

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 are numerous controls in place to ensure data integrity and to prevent unauthorized access. Access is controlled by User Roles, each role assigned gives access only to the data

he/she needs to perform their job. The data is stored in the Data Tier Servers running at the EPA NCC RTP location. All the data is encrypted per the protocol used for the Directory and Data Tier.

eBusiness uses this information in order to provide the means for WCF Activity Managers and Service/Product Managers to accurately provide and charge-back for WCF products and services. eBusiness uses automated registrations, usage submissions, billing, and various reporting features to deliver, manage, and charge for WCF ordered activities across the WCF portfolio.

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

All EPA employees and contractors (internal affiliates) are required to take the Agency Privacy and Information Security Awareness training annually.

All users are required to read and sign the EPA Rules of Behavior that governs the appropriate use of information systems.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

The Privacy and Security Awareness training are run by the Privacy and Security programs. These program offices ensure compliance with training and policies supporting these programs.

Mitigation:

N/A

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 system uses automated registrations, usage submission, billing, and various reporting features to deliver, manage, and charge for WCF ordered services.

eBusiness collects this information in order to deliver Working Capital Fund Services (WCF) to Agency customers (employees and affiliates). Information used is not available for public users or access.

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.)

The registration attributes are made available for use by eBusiness. Personnel having authorized access to eBusiness include the account managers that manage the ordering and registrations in eBusiness. They can search by user name. General person information is retrieved by account managers to manage their services

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

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:

There is no privacy risk. eBusiness is only available to those authorized users. It contains no access to information for use by External Business Partners and is not available for general public use. Authentication is required to log-in. eBusiness collects personal information on users to the extent necessary to establish the necessary accounts needed to shop, order/cancel, monitor, and manage WCF products and services via an on-line catalog. The personal information includes your name, business phone number, business email, business address. The self-registration form will not contain your Social Security number, date of birth, address, description of physical appearance, medical information, or job description. The information stored in eBusiness provides the means for WCF Activity Managers and Service/Product Managers to accurately provide and charge-back for WCF products and services. eBusiness uses automated registrations, usage submissions, billing, and various reporting features to deliver, manage, and charge for WCF ordered activities across the WCF portfolio.

Mitigation:

All the system components for eBusiness are hosted at the NCC in RTP, NC on the internal EPA Network. eBusiness is only accessible to authorized users.

The information that is collected during the Identification process is protected in accordance with the Privacy Act of 1974, as amended and other Federal privacy laws and policies. The information can be accessed only by trusted members of the OASIS team on a need-to-know basis.

*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.

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?

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?

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). 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:

Mitigation: