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: Flexera Data Platform (FDP)	
Preparer: Bryan Hodge	**Office:** OMS-OITO-ECSD
Date: 06/05/20	**Phone:** 919-541-0317
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 Flexera Data Platform (FDP) in an on-premise browser-based software solution that analyzes raw information technology (IT) data for data quality issues, such as terminology variations, conflicts and duplicates, and organizes the data into a more consistent state. Product features include the ability to normalize vendor names, product names and versions, and append market data (e.g. support dates, end-of-life dates, hardware dimensions) to existing repository that enables EPA staff to view this normalized data from other EPA IT discovery sources such as BigFix Inventory (BFI), McAfee ePO, eBusiness, Sunflower and Microsoft System Center Configuration Manager (SCCM). The overall objective of the project is to normalize data from these various EPA data sources and export the data into EPA ServiceNow Configuration Management Database (CMDB).

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?

The legal authorities for the collection of this information are 5 U.S.C. § 301 "Departmental Regulations" and 8 U.S.C § 1101, 1103, 1104, 1201, 1255, 1305, § 3101 "Records Management by Federal Agency Heads."

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?

Flexera Data Platform (FDP) has been added as a subsystem of the Enterprise Services System (ESS). The ESS has a system security plan and a current ATO, which expires December 11, 2020. ESS will undergo a security assessment in June/July of 2020 which will evaluate FDP control compliance.

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?

Flexera Data Platform (FDP) data will not be maintained or stored in a Cloud environment.

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).

Extracted Data Fields That Contain PII	
Custodian	Person Accountable for the Asset
Email Address	Individual assign to asset work email address
User	Assigned Individual to Hardware

Non-PII Extracted Data Fields	
Accountable Area	Steward of Asset
Activity Status	Latest Status of Hardware
Asset Value	Cost of Asset
Boot device	Related to Operating System Image
Building	Hardware Location
Computer DNS Name	Asset Identifier
Computer ID	BigFix Computer ID used in Flexera to help normalize data
Computer Name	Asset Identifier
Computer OS	Operating System Type
CPU Speed	Hardware Data
CPU Type	Hardware Data
Custodial Area	Steward Child/Children of Asset
Decal Number	Asset Identifier
Description	Hardware Model
Discovery Path	BigFix Client Discovery Path
Free Disk Space	Hardware Data
Hard Drive Size	Hardware Data
Hardware Manufacturer	Hardware Brand
IMEI ESN	International Mobile Equipment Identity Electronic serial number to uniquely identify mobile devices
In Production Date	Installation Date
Initial Event	Identifies lease or purchase of hardware
Invoice Date	Purchase date of hardware
IP Address	Asset Identifier
IP Host Name	Asset Identifier
LanID	Assigned EPA short name credentials for identification and authentication
Last Seen	When asset was last discovered in BigFix
MAC Address	Asset Identifier
Model	Hardware Brand Model
Net Address	Asset Identifier
Number of Processors	Hardware Data
Office Name	Users office or department
Operating System	Captures operating system name
OS Version	Version of Operating System (i.e. 2012, 2016 or Windows 10)
PO Number	Purchase order number for asset
Processor Brand	Hardware Data

Processor Vendor	Hardware Data
Product Name	Type of Hardware (Desktop, etc.)
Product Release	Software Version
Receive Date	Date hardware received
Registration ID	Registration ID associated with hardware in eBusiness
Registration Start Date	Date hardware was assigned
Serial number	Hardware Data
SI Number	Computer Vendor Number
Software Product Name	Software Identifier
Software Product Publisher Name	Software Manufacturer Identifier
System Type	Hardware Data
Total Disk Space	Hardware Data
Total Physical Memory	Hardware Data
Total Virtual Memory Size	Hardware Data
Username	Assigned Individual to Hardware
User Property	Program Office or Region Office of Hardware User
VDI	Virtual device or Physical
Warranty End Date	End of hardware warranty date
Windows directory	Hardware Data

The information in the table above is only used to normalize the data from the other EPA data sources in order to help the EPA gain valuable insight into the hardware and software residing within the Agency that will be consistent, complete, accurate and current.

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

The sources of the information in Flexera Data Platform (FDP) comes from BigFix Inventory (BFI), McAfee ePO, eBusiness, Sunflower and Microsoft System Center Configuration Manager (SCCM) using extractor database user accounts that have read-only permissions. No data is collected directly from individuals.

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

FDP does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

FDP leverages Technopedia, the world's largest catalogue of IT product information on more than 90,000 enterprise IT products and patented rule-based mapping to deterministically map data to a common identity and categorize it based on vendor name,

product name, product version and other relevant criteria. Then FDP aaggregates and de-duplicates this normalized data to resolve conflicts and other data quality issues.

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:

There is very small risk related to the quality of the information or data extracted from BigFix Inventory (BFI), McAfee ePO, eBusiness, Sunflower and/or Microsoft System Center Configuration Manager (SCCM). The information extracted may not be totally accurate and can't be verified at the time the data is extracted because it doesn't come directly from individuals but is rather gathered from other EPA data sources.

Mitigation:

While limited to the accuracy of the data extracted from other EPA data sources, one of the main purposes of Flexera Data Platform (FDP) is providing visibility of the EPAs asset inventory ownership. Any inaccurate data extracted from these outside data sources that FDP pulls data from will be reviewed and updated by the system owners often which will help ensure more accurate over time.

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. Logical Access controls are in place for Flexera Data Platform (FDP) console using role-based security access. The types of roles are Platform administrator, Platform read-only, User Console Report Manager, User Console Editor and User Console Viewer. In the EPA there is only the role of platform administrator and it cannot be accessed via EPA LAN credentials, whether privileged or non-privileged, or using a EPA issued PIV card. It can only be accessed using the dedicated Flexera Service Account that is authorized to see all data extracted into the console from these other EPA data sources. These Flexera Data Platform (FDP) Service Account is role-based and managed in the application console.

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

Logical access controls are documented in EPA Flexera Data Platform Design v1.4 April 15, 2020.

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

No. There are no other components with assigned roles and responsibilities.

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?

FDP access is only for internal FDP administrators. Data or information will not be accessible to any external parties (i.e. the public, outside agency, or external companies/contractors).

All appropriate FAR clauses have been included in the ITS-EPA III End User Services (EUS) contract which includes FAR Clauses 52.24.1 Protection of Individual Privacy and 52.24.3 Privacy Training.

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.

Flexera Data Platform (FDP) database information is not retained permanently. The data or information extracted from BigFix Inventory (BFI), McAfee ePO, eBusiness, Sunflower and Microsoft System Center Configuration Manager (SCCM) is not retained in the console. The data information is continuously updated via Restful application program interface (API) that access the latest information and normalizes it. The system follows EPA Records Schedule 0089 Information Tracking System and 1012 Information and Technology Management for database data that is backed up.

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 is a low risk with retention of data beyond the appropriate Records Schedules for FDP.

Mitigation:

This risk is mitigated by following the appropriate Records Schedules 0089 and 1012.

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. Information is not shared outside of EPA as part of the normal agency operations

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

There is no external sharing.

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?

All systems that Flexera Data Platform (FDP) imports data from or exports data into are under the same Chief Information Officer (CIO) and ISO. There are no requirements to have information sharing agreements (ISAs) or Memorandum of Understandings (MOUs). There is no sharing outside the EPA. New information sharing agreements will be managed in accordance with EPA procedure.

4.4 Does the agreement place limitations on re-dissemination?

Not Applicable, there are no 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:

None. No information is shared outside the agency.

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 as stated in Section 6.1?

The system ensures that the information is used as stated in section 6.1 by employing security controls that provides data integrity by using TLS encryption for data in transit and database level encryption on the SQL database. To help prevent unauthorized access. Access is controlled by user-based roles managed in the FDP console. Auditing of user's actions is also captured in the console and captured on the SQL database using EPA PA File Sight.

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

The US EPA implements a Rules of Behavior (ROB) for which all users must consent prior to being granted systems credentials for access. The EPA requires User Information Security and Privacy Awareness Training (ISPAT) to be completed annually and refresher cybersecurity training annually to help educate how to use and management of sensitive data. In addition, ESS personnel must read and sign the ESS Rules of Behavior document that updated annually that provides information regarding privacy.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk of inappropriate audit to account for all PII usage in the FDP system.

Mitigation:

Audit logs will be reviewed frequently by FDP staff

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.

FDP uses information extracted and normalized from multiple EPA data sources to de-duplicate installation data, provide detailed information on EPA IT assets and a structured catalogue of EPA hardware and software all in order to lower compliance risk and drive EPA standards.

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 system isn't designed to gather information by the user. The Flexera Data Platform (FDP) is designed to use extractors to pull the data and dedicated Service Accounts to access the system console where reports can only be generated about the hardware and software within the Agency.
Records are retrieved by asset name as well as the data source.

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?

[The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.]

A review of the system attributes that are extracted BigFix Inventory (BFI), McAfee ePO, eBusiness, Sunflower and Microsoft System Center Configuration Manager (SCCM) into FDP have been fully identified and evaluate the potential effect on the privacy of individuals. Restrictions on access that are limited dedicated Administrative Flexera Service Account maintained in Active Directory by but managed in the FDP console provides role-based administrative controls. Technical controls are in place by providing TLS encryption on data in transit and encryption on the SQL database.

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:

Low risk of inappropriate use of the information extracted into FDP.

Mitigation:

Mitigation is provided by frequent reviews of audit logs by FDP staff.

*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 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: