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: GoAnywhere	
Preparer: Corei Somerville /Niloufar Salour, ISSO	**Office: OMS/OITO/EOD/POB**
Date: 8/14/2024	**Phone: 919-357-0598**
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:
GoAnywhere is a Managed Secured File Transfer Service that streamlines the secure exchange of files between EPA systems, colleagues, partners, research teams, tribes, and support contractors. The types of data transferred by the GoAnywhere service are scientific data, computational data, files, and documents, which may include sensitive data such as CUI, CBI, NSI, SPII, PII, or financial information. Data is stored outside of the GoAnywhere directory structure on a NHS SAN.

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?

- 44 U.S.C. § 3506, Federal Agency Responsibilities;

- Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource;
- 5 U.S.C. 301, Departmental Regulations;
- 40 U.S.C. 1401, the Clinger-Cohen Act; and
- 44 U.S.C. 3541 et seq., Federal Information Security Modernization Act of 2014
- Public Law 107-347: A security plan must be developed and practiced throughout all life cycles of the agency's information systems.

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 GoAnywhere application has been in operation since 2011. GoAnywhere resides within the boundaries of the NHS and is covered under its SSP. GoAnywhere was issued an ATU on 12/12/2022 and is scheduled to be renewed by 12/12/2024.

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).

GoAnywhere traverses information such as SSN, Date of Birth, full legal names, aliases, maiden names, birth dates, dates of death, current and former home addresses, home/cell/business phone numbers, names of family members, current and former neighbors, current and former business associates, other individuals at home or business addresses, current and former employers, work addresses, Taxpayer Identification Numbers, email addresses.

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

system?

The sources of the information can be both internal and external to the Agency. The external and internal sources are EPA colleagues, partners, research teams, tribes and support contractors. The origins of the data are the EPA colleagues, partners, research teams, tribes and support contractors. GoAnywhere is only the conduit for which the information is transferred from point A to point B.

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 is encrypted by the Managed File Transfer Server when it is uploaded by the user. It is encrypted in accordance with FIPS 140-2. Accuracy of the data is ensured via checksum.

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 the risk of LAN ID exposure, also there is the risk of exposure in transit if file is intercepted.

Mitigation:

There is Security Awareness Training to mitigate LAN ID exposure and Full encryption with FIPs 140-2 compliant algorithm is used to mitigate exposure in transit. Also, GoAnywhere application is only accessible via EPA VPN.

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, the system has built-in access controls that allow for the File Transfer System Administrator to grant, revoke, and modify access levels to users based on file transfer area needs. Administrative users can be added and managed only by an Admin User with the Security Officer role. User administrators have the ability to grant normal (non-

administrative) users, also known as Web Users, access to resources available on the file transfer server. The Web User(s) can belong to one or more Web User Groups and will adopt the permissions from any Web User Group to which they belong. A Web User can also be granted individual permissions for various services, files, and folders. IP filters can also be configured to ensure that Web Users are only accessing GoAnywhere from an expected location.

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

The policy and procedure above is part of an SOP that has been approved by the NSOD management. In Addition, as required by procedure, users review/sign the EPA "Rules of Behavior" that affirms each user is knowledgeable of security responsibilities. EPA users undergo internal agency security awareness training.

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

Yes. There are administrative roles. These roles allow administrative access to the GoAnywhere application such as creating projects and adding new users/groups.

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?

Any user with a valid LAN ID whether external or internal can be granted access to the GoAnywhere application. Yes, the appropriate FAR clauses are included in the respective 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.

Data is retained up to 45 days to allow the recipient to accept/download the data. Yes, GoAnywhere has an EPA Records Control Schedule. The EPA RCS is 1012. The records are store in the NHS SAN up to 45 days.

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:

If the recipient's email is compromised the link to the data be accessed by unauthorized party.

Mitigation:

Setting a limit of the number of downloads and enforce the requirement of a password for

download when data contains PII. While the exchanged files may contain PII, all data is fully encrypted in transit.

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 the Agency as part of the normal agency operations. Sharing is between EPA systems, colleagues, partners, research teams, tribes and support contractors. Information is only accessed by permission of the data owner.

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?

N/A

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. There is no external sharing.

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?

GoAnywhere is a Managed Secured File Transfer Service and its purpose is to streamline the secure exchange of files between EPA systems, colleagues, partners, research teams, tribes and support contractors whom maybe external to the organization. While the exchanged files may contain PII, all data is fully encrypted in transit. There is an audit log

capability within GoAnywhere that would allow administrator to track any misuse of data by users.

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

Users must complete annual mandatory training for Information Security and Privacy Awareness.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Unauthorized access to audit logs

Mitigation:

Role based access is strictly enforced. Only authorize admins have access to audit logs.

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.

GoAnywhere is a Managed Secured File Transfer Service and its purpose is to streamline the secure exchange of files between EPA systems, colleagues, partners, research teams, tribes and support contractors whom maybe external to the organization.

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.*)

GoAnywhere is used only to transfer data. The system by design is not meant to retrieve any information therefore there is no retrieval data associated with the system.

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?

GoAnywhere has embedded controls that protect the privacy of individuals who use the system. Only users with the proper credentials can access GoAnywhere. The system restricts broad access of the information uploaded/shared in GoAnywhere. Only the intended recipient can access the data that is sent. All data uploaded into GoAnywhere is encrypted in compliance with FIPS 140-2.

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 a minimal risk of misuse of Data.

Mitigation:

There is an audit trail in place to track system usage.

*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: