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: Bomgar	
Preparer: Liza Hearns and Steve Estes	**Office:** OMS-OITO-ECSD / OMS-OITO-NSOD-NTSB
Date: 09/30/2021	**Phone:** Liza Hearns Ph: 202-566-0759 and Steve Estes Ph: 919-541-2812
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:

Bomgar is a sub application component under Enterprise Services System. Bomgar, a Beyond Trust Inc. remote desktop support application allows EPA helpdesk support staff or technicians to remotely connect to end-user systems through agency firewalls from their computer or mobile device to fix EPA devices or applications. It also allows the helpdesk support personnel to chat with the end-user within the application to help fix problems faster.

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 authority for the collection of this information is defined in:

- 5 U.S.C. 301 (Executive Department regulations);
- 41 CFR 101-35 (Telecommunications Management Policy); and
- 44 U.S.C. 3101 (Records management by agency heads; general duties).

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?

Bomgar is a component application under Enterprise Services System. A system security plan for Enterprise Services System has been completed and has an ATO that expires March 9, 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 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?

Bomgar application 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).

- EPA Email Address
- Customers First Name
- Customers Last Name
- EPA LAN ID

- Workstation Name

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

EPA Active Directory and the customer are the sources of the information collected by Bomgar. Customer first and last name are collected directly from the customer to start the remote assist session. The EPA email address is collected from EPA Active Directory.

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

Bomgar doesn't use any information from commercial sources or publicly available data

2.4 Discuss how accuracy of the data is ensured.

The accuracy of the data in Bomgar is ensured by capturing the EPA LAN ID, first name, last name and computer name from the customers already successfully established EPA network authentication session and once the customer establishes the remote support session utilizing the Bomgar session key this data is automatically generated.

2.5 <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>:

The risk is minimal. There's a small risk that data collected automatically from the customers successfully authenticated EPA network session is inaccurate.

<u>Mitigation</u>:

The customer has the ability to verify and correct their information that is gathered by Bomgar prior to any remote support session.

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. Bomgar uses technical access controls like passwords and application account creation or account roles consisting of Bomgar helpdesk personnel (users) and Bomgar administrators that prevents unauthorized users from accessing information they don't have a need to view. Only Bomgar administrators have access to session data.

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

Procedures for the access controls are documented in the Bomgar Remotes Support Administrator Guide.

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

No. EPA personnel and the contractor are the only users.

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?

Authorized EPA Federal and EPA contractual personnel will have access to this data/information.

The appropriate FAR clauses are included in the contract.

- 52.224-1: Privacy Act Notification
- 52.224-2: Privacy Act
- 52.224-3: 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.

Bomgar session data is retained for 90 days to only provide remote assist data for which helpdesk staff member assisted which customer and when. Longer retention periods aren't available within the Bomgar appliance as it doesn't have a syslog to retain session data longer than 90 days.

Bomgar application follows EPA Records Control Schedule 1012.

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's a risk that this data will be needed to be reviewed after the 90 days retention capabilities currently in place for the Bomgar appliance. Only 90 days of auditing is currently available on the Bomgar appliance and that's a n identified weakness related to retention time. The ability to store data for up to 1 year in Splunk is expected to be in place in FY 2022.

Mitigation:

As a compensating measure for Bomgar because of the lack of the ability of retaining data longer than 90 days, every month, the Bomgar administrators are archiving the oldest 30 days of data in encrypted files until there's at least 1 year of data stored in Splunk.

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.

There is no information shared with any other organization.

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

Not Applicable. There is no information shared with any other organization.

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?

Not Applicable. There is no information shared with any other organization.

4.4 Does the agreement place limitations on re-dissemination?

Not Applicable. There is no information shared with any other organization.

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 information sharing.

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?

Bomgar ensures that the information is only used for its intended purposes by limiting access to the information collected to establish remote assist support. There are technical controls within the Bomgar console and processes in place to prevent unauthorized access. Bomgar access must be granted by the system owner. The Bomgar administrator then adds that user to User Roles within the Bomgar application console. Each role gives access only to Bomgar console in order to start remote assist support. Only users added specifically to Bomgar Administrator Roles have access to session data. Authentication to console uses EPA credentials and passwords.

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

The EPA Information Security and Privacy Awareness Training required by all EPA employees and contractors.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a small risk that Bomgar does not have controls in place that provides the proper safeguarding security measures that can be audited ensuring that users are being held accountable.

Mitigation:

Bomgar archives session data in encrypted files to safeguard against modification online. This data can be used for audit trails of remote support technicians. In addition, users of Bomgar, as well as all EPA employees, must read and acknowledge the EPA Rules of Behavior and complete annual training to maintain access to Bomgar.

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.

Information collected by Bomgar is only to accurately verify the customer and the workstation establishing the remote assist support session.

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.)*

Bomgar application is not designed to retrieve information by users (representatives). User representatives don't have access to old session data.

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?

Bomgar has been configured to reduce access to PII to the user who uploaded it and the administrator. In addition, Bomgar is currently undergoing a full security assessment as part of the ATO which includes a review of all security and privacy controls. Several of these controls are relevant to how Bomgar controls information contained in the application. The system administrators have a layer in depth approach and minimize any privacy risk by following policies and adhering to making sure to update firewall rules daily.

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 small risk that the information collected or stored in Bomgar could be improperly accessed or improperly handled.

Mitigation:

Bomgar data is protected in transit using TLS 1.2 encryption and limited access to the data in the Bomgar console to only administrator roles.

*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: