EPA 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: Tandberg Video Teleconference Infrastructure and Video Teleconferencing (VTCI/VTC)	
Preparer: Herman Hawkins/Mike MCClain	**Office:** OMS/OITO/ECSD
Date:10/2/2020	**Phone: 202-566-1892**
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:

EPA Tandberg Video Teleconference Infrastructure and Video Teleconferencing (VTCI/VTC) system provides the back-office supporting infrastructure required to securely use, manage and maintain the various EPA owned VTC Endpoints that place and receive VTC calls. The VTC Endpoint is a collection of interconnected components such as a camera, microphone, TV and plasma displays and a Coders/Decoders (codec) that comprise of VTC system. These VTC Endpoints are installed in conference rooms and personal offices to allow users to place VTC calls to other endpoints. Examples of VTC endpoints include the Tandberg EX60/90 personal VTC system and the Tandberg MX700 conference room system.

The Tandberg system also consists of Pexip Infinity, which is a self-hosted, virtualized and distributed multipoint conferencing platform. It enables scaling of video, voice and data collaboration across organizations, enabling everyone to engage in high definition video, web, and audio conferencing. Pexip provides any number of users with their own personal Virtual Meeting Rooms, as well as Virtual Auditoriums, which they can use to hold conferences, share presentations, and chat. Participants can join over audio or video from any location using virtually any type of communications tool (such as Microsoft Skype for Business / Lync, a traditional conferencing endpoint, a mobile telephone, or a Pexip Infinity Connect client) for a seamless meeting experience. Pexip Infinity Connect suite of clients allow users to connect to any Virtual Meeting Room or Virtual Auditorium within the Pexip Infinity deployment, either; directly from a web browser without any special downloads or plugins, from an installable desktop client, or from an Infinity Connect mobile client, available for iOS or Android.

The platform also includes the Pexip Distributed Gateway service, which allows end users to place calls to other endpoints that use different protocols and media formats, or to call into an externally hosted conference, such as a Microsoft Teams or Skype for Business meeting.

Pexip Infinity's unique distributed architecture is purely software-based and virtualized, running on industry-standard servers, meaning it can be deployed quickly and simply with the flexibility to scale as required. In addition, the Pexip Infinity platform has been designed to comply with US Federal security requirements.

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?

5 U.S.C. 301, Departmental Regulations; 44 U.S.C. Chapter 35, the Paperwork Reduction Act; 40 U.S.C. 1401, the Clinger-Cohen Act; 44 U.S.C. 3541 et seq., Federal Information Security Modernization Act of 2014; OMB Circular A-130, Managing Information as a Strategic Resource; Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service," April 11, 2011; Presidential Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011; and Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012

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 Tandberg (including PEXIP) is a sub-component and completed as part of the Email and Collaboration Solutions (ECS) system, which is going through its annual assessment and ATO process at this time. The ATO is TBD and scheduled to be acquired in August of 2020.

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?

The data is not maintained or stored in a Cloud.

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).

The system uses a person's name to program a personal video teleconferencing system (VTC) in Tandberg. The system uses a person's name to create a personal Virtual Meeting Room (VMR) in Pexip. The system uses a person's email address to send automatic emails in Pexip.

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

Individual provides information, EPA Locator, O365, and 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.

No

2.4 Discuss how accuracy of the data is ensured.

The accuracy of the data is confirmed with the user of the personal VTC system or personal VMR. This data is not used for dialing other VTC systems or VMRs. The SIP address of the VTC systems and VMRs are used for dialing. A SIP address could contain an users name and in fact it does when it is a personal VTC system or VMR. See Figures 1 and 2 for examples of the SIP address of a personal system and a personal VMR

Due to the nature of the system and the anticipated broad use of VTC across the EPA, it is the responsibility of each user to ensure accuracy of data at the time the system is installed. The Tandberg administrator ensures user information is accurate and for calling numbers from outside unrecognized dialers, the administrator is responsible for writing firewall rules that will block these numbers.

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:

The system potentially could be subject to shoulder surfing or social engineering, which would be of a very low nature, however, a picture or email/names could possibly be given to somebody outside the agency. If a firewall rule is not set up, there could be a potential for a user from a foreign country dialing in to tie up the meeting lines. By default, the system is designed to share information using video teleconferencing communication, however, no information is provided outside of the EPA.

Mitigation:

The information is protected through defense-in-depth security controls and can only be accessed by a few administrators that directly manage and provide limited access for those that have the need to know. Firewall rules are set so that no prank calls can access the system, and nobody can attend the meetings without proper access roles and privileges.

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?

The Tandberg (including PEXIP) is a sub-component and completed as part of the Email and Collaboration Solutions (ECS) system, which is going through its annual assessment and ATO process at this time. All Access controls for this system are defined in the ECS documentation.

The System has fundamental access controls limited to the person dialing and the person receiving the video call. Namely, only the name and email are able to be accessed. These controls give permission for users to use the VTC equipment to access end to end TV and conferencing. Firewall rules are written to prevent access to random or unauthorized callers that try to gather information on the Tandberg system from outside of the agency.

This information is not used for the dialing between VTC systems and VMRs. Physical measures include restrictions on building access to authorized individuals only, and by maintaining records in lockable offices and filing cabinets.

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

Access to names/callers and email information is controlled through Active Directory (AD) and stored within the group folders within the OU container within AD. The policy for rights/privileges are contained and based off the EPA CIO signed New Privileged User Guidance: Account Type Matrix, dated April 3, 2020. Access can be revoked or edited by the site owner using these ACLs. The ACL groups determine the roles and what information can be accessed by which users. Each host of the meeting can provide certain restrictions for who can access the VTC meeting.

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

No

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?

Both government and contractor employees have access to the data/information in Tandberg. The appropriate FAR clauses, CFR 24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act, have been incorporated into the contract and provide a foundation for the contractor's privacy data protection policies.

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 name and email address, when applicable, are retained for as long as the individual has use of a personal VTC system or a personal VMR. This information is retained to provide a means by which VTC systems and VMRs can be managed and maintained. The information is used to manage and maintain the 789 VTC systems installed across the agency and the 688 Pexip VMRs. The information is also used to generate system usage reports on a monthly basis as well as a VTC directory The system is a new sub-system that is a part of the umbrella system ECS, and therefore, does not have a Records Control Schedule at this time, however, the system will request a new RCN as directed (if applicable).

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 any information was retained, it would follow the Capstone Policy for the 10 years period, so relatively low risk, if the time that is retained is not enforced, some data may be accidently purged that may be recent, causing some loss of archived information.

Mitigation:

No information or data containing PII is stored, however, if somebody were to freely steal or record data from any meeting and use it for compromising sensitive information, this would be a violation of the Rules of Behavior and cause an investigation and incident that could potentially cause that person/s to be fired, pay fines, or be subject to criminal litigation. Training, auditing, and other security safeguards are in place. Safeguards include training to administrators on how to use the system and consent to actions and monitoring such as audit trails. Also, the system has several other safeguards such as antivirus controls for any intent to compromise the records and firewall rules to prevent access to unauthorized individuals to change/delete those records.

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, this information is not shared outside the EPA.

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?

Tandberg currently does not have any MOUs or Information Sharing Agreements (ISAs) and no information is shared externally outside of EPA.

4.4 Does the agreement place limitations on re-dissemination?

N/A, there is no agreement for limitations on re-dissemination.

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, information is not shared externally.

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?

EPA ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behaviour, and auditing and accountability. EPA security specifications require auditing capabilities that log the activity of each user to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All EPA systems employ auditing measures and technical safeguards to prevent the misuse of data.

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 Behaviour (ROB) for which all users must consent prior to being granted systems credentials for access. The system inherits the EPA implementation of User Information Security and Privacy Awareness Training (ISAPT) which is provided annually. In addition, all EPA personnel receive annual refresher cybersecurity training to educate them regarding the use and management of sensitive data.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a low risk that an EPA workstations or laptops can be lost or stolen and that an outside entity can steal and impersonate an EPA user by stealing their credentials. Since all hardware and software contain tracking inventory information, the risk of anybody impersonating another EPA user is very low. For any compromised systems or incidents that involve the information within the application, all loss of PII would default back to the user and their workstation.

Mitigation:

At the operating and system level, logs are automatically created, managed and maintained by system administrators. Also, the access to VTC has protective measures in place such as "https" and Single Sign On. Application logs (Successful, Unsuccessful) provide traceability into activity within the EPA network. Admins and users are trained annually on the responsibility of protecting their laptops and complying to password/authentication policy with the EPA.

If a lost or compromised workstation is discovered, all access to the VTC meetings is removed, along with access to the EPA network, making is impossible for any unauthorized person to use the application. System administrators and network admins are responsible for reports generation, analysis, and submittal to stakeholders designated authorized official(s).

All account-related functions are audited and stored according to EPA policy and is NIST 800-53 Rev. 4 compliant.

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 the information to program a personal VTC system or to create and program a personal VMR. information to manage and maintain VTC systems and Pexip VMRs. The information is also used to generate system usage reports on a monthly basis as well as a system directory.

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 information can only be accessed and retrieved by system administrators with **authorized** access defined in Access Controls in the ECS system. The connection, in order to use the VTC devices are connected to audio/video by the SIP address of the VTC system or VMR. No PII is stored within the system.

The system is designed as a video teleconference application and cannot be retrieved. PII is not stored and cannot be retrieved by a personal identifier for any user. Only administrators can retrieve the information and only by System Name, which does not contain PII in this case.

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 EPA is currently undergoing an assessment for all security controls within a larger system known as Email and Collaboration (ECS), which has tested several security controls within Tandberg relating to Privacy. Several of these controls are relevant to how Tandberg shares information and controls that information. 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. Also, by the careful analysis of the system, the EPA has provided several security tools that filter out data and help to prevent security leakage and privacy information from being compromised. Some of the tools include: Data Loss Prevention, Valimail, Advanced Data Protection, and as mentioned in this document Access Control Lists (ACLs). In this way, the EPA has allowed these tools and services to prevent PII exposure and limit access to unauthorized individuals.

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 low risk of misuse of the system, for example if an administrator directly or indirectly shares information about the system and provides a name or phone number of an individual or information that could allow an individual to receive information that is not meant to be shared.

Mitigation:

Tandberg restricts all information based on business need by role-based access control, multifactor authentication, and minimal access controls. Any VTC meetings from unauthorized users are strictly forbidden. Access to customer data is also strictly logged and third parties perform annual assessments and audits (as well as sample audits) to attest that all access controls are meeting EPA's requirement and are appropriate.

***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: