Template Version Number: 01-2021

# U.S. Department of Commerce
# U.S. Patent and Trademark Office

## Privacy Impact Assessment
## for the
## Zoom For Government (ZFG)

Reviewed by: Henry J. Holcombe, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 3/9/2022

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

# U.S. Department of Commerce Privacy Impact Assessment
# USPTO Zoom For Government (ZFG)

**Unique Project Identifier: EIPL-EUS-06-00**

## Introduction: System Description

*Provide a brief description of the information system.*

The Zoom for Government (ZfG) Platform is a Zoom product offering for the US Federal community and the international community. The platform unifies cloud video conferencing, simple online meetings, and a software-defined conference room into one solution. The platform can be used for an international audience by various business units. It also provides video, audio, and wireless screen-sharing across Windows, Mac, Linux, Chrome Operating System (OS), Internetwork Operating System (iOS), Android, BlackBerry, Zoom Rooms, and Internet Protocol signaling standards H.323/SIP room systems. The ZFG products include:

**Zoom Cloud Video Conferencing** – a cloud-based collaboration service which includes video, audio, content sharing, chat, webinar, cloud recording and collaboration.

**Zoom Rooms** – software-based group video conferencing for conference and huddle rooms that run off-the-shelf hardware including a dedicated Macintosh (MAC) or personal computer (PC), camera, and speaker with an iPad controller.

**Zoom API** – provides the ability for developers to easily add Video, Voice and Screen Sharing to your application. Zoom's application platform interface (API) is a server-side implementation designed around Representational State Transfer (REST). The Zoom API helps manage the pre-meeting experience such as creating, editing, and deleting resources like users, meetings and webinars.

**Zoom Phone** – modern, cloud-based phone system that is available as an add-on to Zoom's video communications suite.

**Zoom Client** – allows users to start/join a meeting, employ in-meeting controls for participants, hosts, and co-hosts, webinar controls, manage participants, share screen controls, update profiles, chat, establish channels, add contacts, and modify settings.

Address the following elements:

***(a) Whether it is a general support system, major application, or other type of system***
ZFG is a Software as a Service (SaaS).

***(b) System location***
ZFG is in the ZFG FedRAMP SaaS cloud managed platform.

***(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)***
ZFG is a standalone system and does not interconnect with any other systems.

***(d) The way the system operates to achieve the purpose(s) identified in Section 4***

The host, or user that schedules the meeting, logs into ZFG Federal Risk and Authorization Management Program (FedRAMP) managed platform SaaS cloud via a web browser client. The host then opens the scheduler window to select meeting settings to include the topic, date and time, meeting identification (ID), security, encryption, video, and audio for example. Once the meeting settings are saved, the system will generate the meeting invite. The host can then invite pre-determined participants to the ZFG meeting via the system generated meeting invite link. Security settings include creating a meeting passcode that participants will be required to input before joining the meeting, *Waiting Room*, which enables the waiting room for the meeting, and *Only authenticated users can join*, a feature that restricts access to the meeting so that only signed-in users can join. Encryption options include a choice between the standard enhanced encryption (encryption keys stored in the cloud) and End-to-end encryption (encryption keys stored on a local device) for the meeting.

***(e) How information in the system is retrieved by the user***

A host is required to authenticate, via Hypertext Transfer Protocol Secure (HTTPS), to the Zoom site with their user credentials such as user ID and password or single-sign-on (SSO). Information is then retrieved from the system via a secure Internet connection to the ZFG FedRAMP Managed Platform SaaS Cloud.

***(f) How information is transmitted to and from the system***

ZFG follows strict guidelines regarding handling and transmitting information. Data transmitted to and from ZFG is protected by secure methodologies such as HTTPS, used for secure communication over a computer network and Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security 1.2 (TLS 1.2). Security Assertion Markup Language 2.0 (SAML 2.0) is used for exchanging authentication and authorization identities between security domains. All data stored at rest is also encrypted.

***(g) Any information sharing conducted by the system***

ZFG will share information within the bureau via case-by-case, bulk transfer, and direct access.

***(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information***

5 U.S.C 301, 35 U.S.C. 2, E.O.12862, and E-Government Act provide the authority for collecting, maintaining, using, and disseminating information in ZFG.

***(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system***

The FIPS 199 security impact category for the system is Moderate.

## Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☒ This is a new information system.

☐ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

| Changes That Create New Privacy Risks (CTCNPR) | | | | | |
|---|---|---|---|---|---|
| a. Conversions | ☐ | d. Significant Merging | ☐ | g. New Interagency Uses | ☐ |
| b. Anonymous to Non-Anonymous | ☐ | e. New Public Access | ☐ | h. Internal Flow or Collection | ☐ |
| c. Significant System Management Changes | ☐ | f. Commercial Sources | ☐ | i. Alteration in Character of Data | ☐ |
| j. Other changes that create new privacy risks (specify): | | | | | |

☐ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

## Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

| Identifying Numbers (IN) | | | | | |
|---|---|---|---|---|---|
| a. Social Security* | ☐ | f. Driver's License | ☐ | j. Financial Account | ☐ |
| b. Taxpayer ID | ☐ | g. Passport | ☐ | k. Financial Transaction | ☐ |
| c. Employer ID | ☐ | h. Alien Registration | ☐ | l. Vehicle Identifier | ☐ |
| d. Employee ID | ☐ | i. Credit Card | ☐ | m. Medical Record | ☐ |
| e. File/Case ID | ☐ | | | | |
| n. Other identifying numbers (specify): | | | | | |
| *Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: | | | | | |

| General Personal Data (GPD) | | | | | |
|---|---|---|---|---|---|
| a. Name | ☒ | h. Date of Birth | ☐ | o. Financial Information | ☐ |
| b. Maiden Name | ☐ | i. Place of Birth | ☐ | p. Medical Information | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| c. Alias | ☐ | j. Home Address | ☐ | q. Military Service | ☐ |
| d. Gender | ☐ | k. Telephone Number | ☐ | r. Criminal Record | ☐ |
| e. Age | ☐ | l. Email Address | ☒ | s. Marital Status | ☐ |
| f. Race/Ethnicity | ☐ | m. Education | ☐ | t. Mother's Maiden Name | ☐ |
| g. Citizenship | ☐ | n. Religion | ☐ | | |
| u. Other general personal data (specify): | | | | | |

| **Work-Related Data (WRD)** | | | | | |
|---|---|---|---|---|---|
| a. Occupation | ☐ | e. Work Email Address | ☒ | i. Business Associates | ☐ |
| b. Job Title | ☐ | f. Salary | ☐ | j. Proprietary or Business Information | ☐ |
| c. Work Address | ☐ | g. Work History | ☐ | k. Procurement/contracting records | ☐ |
| d. Work Telephone Number | ☐ | h. Employment Performance Ratings or other Performance Information | ☐ | | |
| l. Other work-related data (specify): | | | | | |

| **Distinguishing Features/Biometrics (DFB)** | | | | | |
|---|---|---|---|---|---|
| a. Fingerprints | ☐ | f. Scars, Marks, Tattoos | ☐ | k. Signatures | ☐ |
| b. Palm Prints | ☐ | g. Hair Color | ☒ | l. Vascular Scans | ☐ |
| c. Voice/Audio Recording | ☒ | h. Eye Color | ☒ | m. DNA Sample or Profile | ☐ |
| d. Video Recording | ☒ | i. Height | ☐ | n. Retina/Iris Scans | ☐ |
| e. Photographs | ☒ | j. Weight | ☐ | o. Dental Profile | ☐ |
| p. Other distinguishing features/biometrics (specify): | | | | | |

| **System Administration/Audit Data (SAAD)** | | | | | |
|---|---|---|---|---|---|
| a. User ID | ☒ | c. Date/Time of Access | ☒ | e. ID Files Accessed | ☐ |
| b. IP Address | ☐ | f. Queries Run | ☐ | f. Contents of Files | ☐ |
| g. Other system administration/audit data (specify): | | | | | |

| **Other Information (specify)** |
|---|
| |
| |

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

| **Directly from Individual about Whom the Information Pertains** | | | | | |
|---|---|---|---|---|---|
| In Person | ☐ | Hard Copy: Mail/Fax | ☐ | Online | ☒ |
| Telephone | ☐ | Email | ☐ | | |

| Other (specify): |
|---|

| **Government Sources** | | | | | |
|---|---|---|---|---|---|
| Within the Bureau | ☒ | Other DOC Bureaus | ☒ | Other Federal Agencies | ☒ |
| State, Local, Tribal | ☒ | Foreign | ☒ | | |
| Other (specify): | | | | | |

| **Non-government Sources** | | | | | |
|---|---|---|---|---|---|
| Public Organizations | ☒ | Private Sector | ☒ | Commercial Data Brokers | ☐ |
| Third Party Website or Application | | | ☐ | | |
| Other (specify): | | | | | |

2.3 Describe how the accuracy of the information in the system is ensured.

| ZFG is secured using appropriate administrative, physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, auditing). Mandatory information technology (IT) Awareness and role-based training is required for staff who have access to the system and addresses how to handle, retain, and dispose of data. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access and changes as part of verifying the integrity of data. Security settings include creating a meeting passcode that participants will be required to input before joining the meeting, Waiting Room, which enables the waiting room for the meeting, and only authenticated users can join, a feature that restricts access to the meeting so that only signed-in users can join. Encryption options include a choice between the standard enhanced encryption (encryption keys stored in the cloud) and end-to-end encryption (encryption keys stored on a local device) for the meeting. |
|---|

2.4 Is the information covered by the Paperwork Reduction Act?

| ☐ | Yes, the information is covered by the Paperwork Reduction Act.<br>Provide the OMB control number and the agency number for the collection. |
|---|---|
| ☒ | No, the information is not covered by the Paperwork Reduction Act. |

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

| **Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)** | | | |
|---|---|---|---|
| Smart Cards | ☐ | Biometrics | ☐ |
| Caller-ID | ☐ | Personal Identity Verification (PIV) Cards | ☐ |
| Other (specify): | | | |

| | |
|---|---|
| ☒ | There are not any technologies used that contain PII/BII in ways that have not been previously deployed. |

## Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

| Activities | | | |
|---|---|---|---|
| Audio recordings | ☒ | Building entry readers | ☐ |
| Video surveillance | ☐ | Electronic purchase transactions | ☐ |
| Other (specify): Video recordings | | | |

| | |
|---|---|
| ☐ | There are not any IT system supported activities which raise privacy risks/concerns. |

## Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

| Purpose | | | |
|---|---|---|---|
| For a Computer Matching Program | ☐ | For administering human resources programs | ☐ |
| For administrative matters | ☒ | To promote information sharing initiatives | ☒ |
| For litigation | ☐ | For criminal law enforcement activities | ☐ |
| For civil enforcement activities | ☐ | For intelligence activities | ☐ |
| To improve Federal services online | ☒ | For employee or customer satisfaction | ☒ |
| For web measurement and customization technologies (single-session) | ☐ | For web measurement and customization technologies (multi-session) | ☐ |
| Other (specify): | | | |

## Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

ZFG collects information about Department of Commerce (DOC) employees, contractors working on behalf of DOC, other federal government personnel, and members of the public for administrative matters, to improve federal services online, to promote information sharing initiatives, and for employee and customer satisfaction. ZFG provides a virtual meeting space whereby participants such as employees and USPTO customers can exchange information. ZFG virtual meetings help USPTO bring their teams together in an environment that is easy to use, reliable, and accessible in the cloud. Participants can use video, voice, content sharing, and chats across a variety of devices including mobile, desktops, telephones, and room systems. Audio and video recordings will be used to recall and share meeting data. ZFG is also secure, with a variety of security features that can be enabled at the time of meeting creation via settings. Security settings include creating a meeting passcode that participants will be required to input before joining the meeting, Waiting Room, which enables the waiting room for the meeting, and Only authenticated users can join, a feature that restricts access to the meeting so that only signed-in users can join. Encryption options include a choice between the standard enhanced encryption (encryption keys stored in the cloud) and End-to-end encryption (encryption keys stored on a local device) for the meeting.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats to privacy include foreign entities, insider threats, compromised credentials, missing or poor encryption, and misconfiguration etc.. ZFG implements security and management controls to prevent and mitigate these potential threats to privacy. Management controls such as access control policies and procedures and automated audit actions, for example. Audit actions are when the system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies the appropriate USPTO personnel. ZFG uses privileged user accounts, established based on user roles and separation of duties. Separation of duties means that no one person has sole control over the lifespan of an action. This prevents errors and fraud. USPTO enables least privilege and session lock. Least privilege authorizing access to users only when necessary. Session lock is when the system automatically locks the workstation after 15 minutes of inactivity. In addition, users are provided one-on-one, weekly, and monthly training. Data transmitted to and from ZFG is protected by secure methodologies such as HTTPS, used for secure communication over a computer network and Internet. In HTTPS, the communication protocol is encrypted using TLS 1.2. SAML 2.0 is used for exchanging authentication and authorization identities between security domains. All data stored at rest is also encrypted.

USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The following are current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

## Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

| Recipient | How Information will be Shared | | |
|---|---|---|---|
| | Case-by-Case | Bulk Transfer | Direct Access |
| Within the bureau | ☒ | ☒ | ☒ |
| DOC bureaus | ☐ | ☐ | ☐ |
| Federal agencies | ☐ | ☐ | ☐ |
| State, local, tribal gov't agencies | ☐ | ☐ | ☐ |
| Public | ☐ | ☐ | ☐ |
| Private sector | ☐ | ☐ | ☐ |
| Foreign governments | ☐ | ☐ | ☐ |
| Foreign entities | ☒ | ☐ | ☐ |
| Other (specify): | ☐ | ☐ | ☐ |

| | |
|---|---|
| ☐ | The PII/BII in the system will not be shared. |

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

| | |
|---|---|
| ☐ | Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII. |
| ☐ | No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII. |
| ☒ | No, the bureau/operating unit does not share PII/BII with external agencies/entities. |

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

| | |
|---|---|
| ☐ | Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.<br>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: |
| ☒ | No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. |

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

| **Class of Users** |
|---|

| | | | |
|---|---|---|---|
| General Public | ☐ | Government Employees | ☒ |
| Contractors | ☒ | | |
| Other (specify): | | | |

## Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

| | | |
|---|---|---|
| ☒ | Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9. | |
| ☒ | Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.zoomgov.com/privacy____. | |
| ☒ | Yes, notice is provided by other means. | Specify how: https://www.uspto.gov/privacy-policy |
| ☐ | No, notice is not provided. | Specify why not: |

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

| | | |
|---|---|---|
| ☒ | Yes, individuals have an opportunity to decline to provide PII/BII. | Specify how: Yes, members of the public can decline to provide PII. Members choose the data they want to provide and USPTO does not verify data that is provided. |
| ☒ | No, individuals do not have an opportunity to decline to provide PII/BII. | Specify why not: USPTO employees and contractors do not have the opportunity to decline to provide PII because they use Single sign on (SSO) through Role-based access control (RBAC) and do not have an opportunity to decline to provide PII. |

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

| | | |
|---|---|---|
| ☒ | Yes, individuals have an opportunity to consent to particular uses of their PII/BII. | Specify how: Yes, members of the public have an opportunity to consent to uses of their PII/BII. Submitting personal information is voluntary. When a user voluntarily submits information, it constitutes their consent for the use of the information for the purposes stated at the time of collection. |
| ☒ | No, individuals do not have an opportunity to consent to particular uses of their PII/BII. | Specify why not: USPTO employees and contractors do not have the opportunity to consent to particular uses of their PII. They use SSO through RBAC and do not have an opportunity to consent to uses of PII. |

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

| | | |
|---|---|---|
| ☒ | Yes, individuals have an opportunity to review/update PII/BII pertaining to them. | Specify how: Yes, members of the public may exercise any of their rights as to personal data controlled by Zoom by sending a request to privacy@zoom.us. USPTO employees and contractors may update their PII held in their account profile and preferences by logging into ZFG. |
| ☐ | No, individuals do not have an opportunity to review/update PII/BII pertaining to them. | Specify why not: |

## Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

| | |
|---|---|
| ☐ | All users signed a confidentiality agreement or non-disclosure agreement. |
| ☐ | All users are subject to a Code of Conduct that includes the requirement for confidentiality. |
| ☒ | Staff (employees and contractors) received training on privacy and confidentiality policies and practices. |
| ☒ | Access to the PII/BII is restricted to authorized personnel only. |
| ☒ | Access to the PII/BII is being monitored, tracked, or recorded.<br>Explanation: Audit logs. |
| ☒ | The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.<br>Provide date of most recent Assessment and Authorization (A&A): _____<br>☒ This is a new system. The A&A date will be provided when the A&A package is approved. |
| ☒ | The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. |
| ☒ | NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M). |
| ☒ | A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks. |
| ☒ | Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy. |
| ☐ | Contracts with customers establish DOC ownership rights over data including PII/BII. |
| ☐ | Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers. |
| ☐ | Other (specify): |

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

| |
|---|
| PII in ZFG is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, regulations, and standards. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorize personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access. Additionally, ZFG is secured by various USPTO infrastructure components, including USPTO established technical controls that includes end-to-end transport layer protocols and where applicable data-at-rest and in-transit encryption. |

## Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

☒ Yes, the PII/BII is searchable by a personal identifier.

☐ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

| | |
|---|---|
| ☒ | Yes, this system is covered by an existing system of records notice (SORN).<br>Provide the SORN name, number, and link. *(list all that apply)*:<br><br>• COMMERCE/DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs<br>• COMMERCE/PAT-TM-19, Dissemination Events and Registrations<br>• COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies<br>• COMMERCE/DEPT-20, Biographical Files and Social Networks |
| ☐ | Yes, a SORN has been submitted to the Department for approval on (date). |
| ☐ | No, this system is not a system of records and a SORN is not applicable. |

## Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

| | |
|---|---|
| ☒ | There is an approved record control schedule.<br>Provide the name of the record control schedule:<br><br>• GRS 5.1, item 020: Non-recordkeeping copies of electronic records |

| | |
|---|---|
| | • GRS 5.2, item 020: Intermediary Records |
| ☐ | No, there is not an approved record control schedule.<br>Provide the stage in which the project is in developing and submitting a records control schedule: |
| ☒ | Yes, retention is monitored for compliance to the schedule. |
| ☐ | No, retention is not monitored for compliance to the schedule. Provide explanation: |

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

| **Disposal** | | | |
|---|---|---|---|
| Shredding | ☐ | Overwriting | ☐ |
| Degaussing | ☐ | Deleting | ☒ |
| Other (specify): | | | |

## Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

| | |
|---|---|
| ☒ | Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. |
| ☐ | Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. |
| ☐ | High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

| | | |
|---|---|---|
| ☒ | Identifiability | Provide explanation: ZFG collects, maintains, or disseminates PII about USPTO employees, other federal employees, contractors, and members of the public. The type of information such as email address, first name, and last name, etc. when combined may uniquely identify an individual. |
| ☒ | Quantity of PII | Provide explanation: The quantity of PII is based on several factors but the primary driver of the amount of data will be based on the number of users accessing and creating an account on the site and the quantity of data shared. USPTO has 10 licensed accounts that can host online meetings. |
| ☒ | Data Field Sensitivity | Provide explanation: The combination of email address, first |

| | | |
|---|---|---|
| | | name, and last name together can identify a particular person especially if the audio and/or video recording is also available. |
| ☒ | Context of Use | Provide explanation: The email address, first name, and last name collected will be used primarily for account creation and logging into the system. Audio and video recordings will shared on a need to know basis if requested. |
| ☒ | Obligation to Protect Confidentiality | Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected accordance to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information. In accordance with the Privacy Act of 1974, PII must be protected. |
| ☒ | Access to and Location of PII | Provide explanation: Access to ZFG is limited to authorized USPTO employees and contractors. The PII is secured using appropriate administrative, physical, and technical safeguards in accordance with FedRAMP SaaS Authorization. ZFG does not disseminate PII information to any other systems. |
| ☐ | Other: | Provide explanation: |

## Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

| |
|---|
| Foreign and adversarial entities, insider threats, and computer failure are activities which may raise privacy concerns related to the collection, maintenance, and dissemination of PII. USPTO has implemented a baseline of security controls to mitigate the risk to information to an acceptable level. USPTO mitigates such threats through mandatory training for system users regarding appropriate handling of information and automatic purging of information in accordance with the retention schedule. |

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

| | |
|---|---|
| ☐ | Yes, the conduct of this PIA results in required business process changes.<br>Explanation: |
| ☒ | No, the conduct of this PIA does not result in any required business process changes. |

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

| | |
|---|---|
| ☐ | Yes, the conduct of this PIA results in required technology changes.<br>Explanation: |
| ☒ | No, the conduct of this PIA does not result in any required technology changes. |

# Points of Contact and Signatures

**System Owner**
Name: Randall (Randy) Hill
Office: Collaborative Services Division (I/CSD)
Phone: (571) 272-8983
Email: Randy.Hill@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Hill, Randy Digitally signed by Users, Hill, Randy Date: 2022.02.16 19:03:46 -05'00'

Date signed: _____

**Chief Information Security Officer**
Name: Don Watson
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-8130
Email: Don.Watson@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2022.02.18 10:48:35 -05'00'

Date signed: _____

**Privacy Act Officer**
Name: Ezequiel Berdichevsky
Office: Office of General Law (O/GL)
Phone: (571) 270-1557
Email: Ezequiel.Berdichevsky@uspto.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2022.02.16 17:43:30 -05'00'

Date signed: _____

**Bureau Chief Privacy Officer and Authorizing Official**

Name: Henry J. Holcombe
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-9400
Email: Jamie.Holcombe@uspto.gov

I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.

Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2022.02.18 12:36:16 -05'00'

Date signed: _____

**Co-Authorizing Official**
Name: N/A
Office: N/A
Phone: N/A
Email: N/A

I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.

Signature: _____

Date signed: _____

**This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.**