Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Zoom For Government (ZFG)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Zoom For Government (ZFG)

Unique Project Identifier: EIPL-EUS-06-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.* The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The Zoom for Government (ZfG) Platform is a Zoom product offering for the US Federal community and 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 cohosts, 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 Federal Risk and Authorization Management Program (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 purpose that the system is designed to serve

The purpose of the system is to provide USPTO business units the capability to meet and collaborate with persons both internal and external to the USPTO via video conferencing.

e) *The way the system operates to achieve the purpose*

The host, or user that schedules the meeting, logs into ZFG FedRAMP managed platform SaaS cloud via a web browser client. The host then opens the scheduler window to select meeting settings, 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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

ZFG collects participant email address, provided username, and stores recorded video and audio when enabled. Participants may include Department of Commerce (DOC) employees, contractors working on behalf of DOC, other Federal Government personnel, and members of the public.

g) Identify individuals who have access to information on the system

The individuals who have access to the information on the system include the ZFG Account Owner, Admins, and Members (hosts).

h) 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 identification (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.

i) 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 of identities between security domains. All data stored at rest is also encrypted.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

☐ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☐ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☒ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☒ Yes. *(Check all that apply.)*

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

□ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

□ Yes, the IT system collects, maintains, or disseminates BII.

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

☒ DOC employees
☒ Contractors working on behalf of DOC
☒ Other Federal Government personnel
☒ Members of the public

□ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ The criteria implied by one or more of the questions above **apply** to the Zoom For Government (ZFG) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

☐ The criteria implied by the questions above **do not apply** to the Zoom For Government (ZFG) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: He, Gengshu Scott Office: Collaborative Services Division (I/CSD) Phone: (571) 272-0038 Email: Ghe@@uspto.gov Signature: Scott G He Digitally signed by Scott G He Date: 2023.02.14 20:22:01 -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 Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2023.02.16 19:40:12 -05'00' Date signed: ________________
Privacy Act Officer Name: Caitlin Trujillo Office: Office of General Law (O/GL) Phone: (571) 270-7834 Email: Caitlin.Trujillo@uspto.gov Signature: Users, Trujillo, Caitlin Digitally signed by Users, Trujillo, Caitlin Date: 2023.02.14 13:46:02 -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 Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2023.02.21 09:16:10 -05'00' Date signed: ________________
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: ________________ Date signed: ________________	