Date of Approval: **August 28, 2020**

PIA ID Number: **5225**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Zoom Gov Proof of Concept, ZoomGov

Is this a new system?

Yes

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

The system does not report to an ESC or governance board.

Current ELC (Enterprise Life Cycle) Milestones:

Vision & Strategy/Milestone 0

Is this a Federal Information Security Management Act (FISMA) reportable system?

No

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

Zoom is a Web conferencing application that will allow both internal IRS Employees and other external parties Chat, share content, share files, have breakout room/sessions, wait in the lobby, screen sharing, whiteboard, Q&A polling, and hand raising. As a Coronavirus emergency mitigation, the Tax Court would like to commence virtual trials using the Zoom for Government platform. Also, as a Coronavirus mitigation, Merit Systems Protection Board (MSPB) judges have begun issuing orders to hold virtual hearings using Zoom for Government. Chief Counsel participation in these legal proceedings, on the court-specified platform, is mandatory. This will allow Chief Counsel to conduct the necessary training on the Zoom for Government product, prepare witnesses to testify remotely over the Zoom for Government product, and to hold meetings with IRS and external litigation stakeholders." This proof of concept will allow Chief Counsel to: Conduct the necessary training on the Zoom for Government product Prepare witnesses to testify remotely over the Zoom for Government product Hold mock trials with IRS and external litigation stakeholders All of the above activities will include IRS and non-IRS participants.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e. last 4 digits, etc.)?

No

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

E-mail Address

Standard Employee Identifier (SEID)

Biometric Identifiers

Employment Information

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List

Official Use Only (OUO) or Limited Official Use (LOU) Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

With the Zoom Gov application, it will be required to have the Zoom Uniform Resource Locator (URL)s Whitelisted so that IRS employees will be able to access the Zoom for Government website. The Zoom application will also be a cloud hosted service. This will allow Chief Counsel to conduct the necessary training on the Zoom for Government product, prepare witnesses to testify remotely over the Zoom for Government product, and to hold meetings with IRS and external litigation stakeholders.

How is the SBU/PII verified for accuracy, timeliness and completion?

The office of Chief Counsel is responsible for the accuracy, timeliness and completeness.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 00.001 Correspondence Files and Correspondence Control Files

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

Yes

Briefly explain how the system uses the referenced technology.

The non-IRS users will be able to login to the zoom web conference through their smartphone or workstations. They will login to the session by providing their username and PIN. IRS users will be able to access the Zoom web conferencing through Single Sign On (SSO).

Does the system use cloud computing?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified

4/29/2019

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

What is the background check level required for CSP?

Moderate

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage

Transmission

Maintenance

Does this system/application interact with the public?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Not Applicable

Please explain.

As per an email from Information Technology(IT)shared by PCLIA Preparer, from IT the response is not applicable because: Zoom for Government (ZfG) as a Collaborative software program does not fall within the scope of Digital Identity Risk Assessment (DIRA) because the platform: o enables open-nature communications which do not resolve a specific business purpose (e.g., process returns, collect PII/6103, resolve audit activities) o The â€˜meeting' organizer (or owner of a collaborative session) controls the admission of participants if the session is not fully open o utilizes standard identity proofing and authentication processes set by the software provider, not the IRS Collaborative software programs utilized by the IRS should have defined rules of behavior to address security policy and procedures and access controls. Instances may occur where a DIRA is required for a collaborative software capability that requires secure authentication. Thus, reach out to DIRA mailbox when there are any changes to ZfG to re-evaluate the DIRA requirement.

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

The Office of Chief Counsel is responsible for notifications to individuals.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

Individual can refuse via email or video.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

These proceedings are conducted pursuant to court order and due process is an inherent part of the litigation process, subject to further orders of court, appeal rights, etc.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated)

IRS Owned and Contractor Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Administrator

IRS Contractor Employees

Contractor System Administrators: Administrator

How is access to SBU/PII determined and by whom?

Role based access would be a Chief Counsel determination using the online 5081 process.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

No

You must work with the IRS Records and Information Management (RIM) Program Office to address records retention requirements before you dispose of any records in this system.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

FedRAMP accredited Third Party Assessment Organizations (3PAOs) perform the initial and periodic assessments of cloud systems to ensure they meet FedRAMP security requirements as part of a Cloud Service Provider's (CSPs) FedRAMP authorization. CSPs partner with 3PAOs for authorizations for each of the three security baselines: Low, Moderate, and High. The FedRAMP Security Threat Analysis was completed by Chief Counsel, in lieu of the SA&A. The Business Unit will complete a SA&A during the ELC Process for the Zoom for Government Enterprise. PCLIA #5225 was only the Zoom Proof of Concept.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

No

When is the test plan scheduled for completion?

7/15/2020

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

The IRS will be provided a Web Link from Zoom in order to access the application.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: Under 100,000

Other: Yes

Identify the category of records and the number of corresponding records (to the nearest 10,000).

Taxpayer records and employee records 10,000+

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent?

Yes

Does the system have a process in place to account for such disclosures in compliance with IRC §6103(p) (3) (A) or Subsection (c) of the Privacy Act? Contact Disclosure to determine if an accounting is required.

Yes