Date of Approval: **October 29, 2020**

PIA ID Number: **5564**

SYSTEM DESCRIPTION

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

Enterprise Zoom for Government, ZoomGov

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Zoom Gov Enterprise, ZoomGov, 1

What is the approval date of the most recent PCLIA?

8/28/2020

Changes that occurred to require this update:

New Interagency Use

Were there other system changes not listed above?

No

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

User and Network Services (UNS)Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

Project Initiation/Milestone 1

Domain Architecture/Milestone 2

Operations & Maintenance (i.e. system is currently operational)

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

Yes

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.

Due to the current COVID-19 pandemic, the IRS has needed a tool that will allow for both internal IRS employees and other external parties to collaborate. The ZoomGov collaboration tool meets this demand and can support the following functions: video and audio sharing, chat windows, application sharing, breakout rooms, wait in the lobby, record meetings, whiteboard, Q&A polling, hand raising, dial-in option, along with meeting and attendance reports. ZoomGov is a feature rich web-based application that will be the interim solution until Microsoft Teams is put into production.

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.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

When there is no reasonable alternative means for meeting business requirements

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)

The ZoomGov application is a web-based tool that supports teleconferencing services with individuals outside of the IRS. No specific PII data is generated or stored by the system during a ZoomGov session. However, the potential exists for a participant in the ZoomGov session to discuss PII / sensitive data. It is also possible that presenters may share presentation materials and other applications / artifacts that display PII / sensitive data. Screen capture and 3rd party recording tools may be used by meeting participants to collect information shared via ZoomGov. To help mitigate unauthorized disclosure of PII and SBU data from a technical perspective, some features have been disabled, such as screen sharing, virtual backgrounds, and file transfers. Though screen sharing is blocked, application sharing is available to all users in the ZoomGov session.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

No specific PII data is generated or stored by the system during a ZoomGov session. However, the potential exists for a participant in the ZoomGov session to discuss PII / sensitive data. It is also possible that presenters may share presentation materials and other applications / artifacts that display PII / sensitive data. Screen capture and 3rd party recording tools may be used by meeting participants to collect information shared via ZoomGov. To help mitigate unauthorized disclosure of PII and SBU data from a technical perspective, some features have been disabled, such as screen sharing, virtual backgrounds, and file transfers. Though screen sharing is blocked, application sharing is available to all users in the ZoomGov session.

Employer Identification Number

Other Taxpayer Identification Number

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

Mailing address

Phone Numbers

E-mail Address

Date of Birth

Place of Birth

Standard Employee Identifier (SEID)

Mother's Maiden Name

Internet Protocol Address (IP Address)

Criminal History

Medical Information

Certificate or License Numbers

Vehicle Identifiers

Passport Number

Financial Account Numbers

Photographic Identifiers

Biometric Identifiers

Employment Information

Tax Account Information

Centralized Authorization File (CAF)

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

Agency Sensitive Information   Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

Procurement sensitive data   Contract proposals, bids, etc.

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.

Proprietary data   Business information that does not belong to the IRS

Protected Information   Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government

Physical Security Information   Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities

Criminal Investigation Information   Information concerning IRS criminal investigations or the agents conducting the investigations.

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

Yes

Describe the other types of SBU/PII that are applicable to this system.

Federal Tax Information

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)

SSN for tax returns and return information is Internal Revenue Code Section 6109

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 USC

PII about individuals for Bank Secrecy Act compliance 31 USC

Information by CI for certain money laundering cases may be 18 USC

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.

ZoomGov is a web-based conferencing collaboration tool. No specific PII data is generated or stored by the system during a ZoomGov session. However, the potential exists for a participant in the ZoomGov session to discuss PII / sensitive data. It is also possible that presenters may share presentation materials and other applications / artifacts that display PII / sensitive data. Screen capture and 3rd party recording tools may be used by meeting participants to collect information shared via ZoomGov.

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

There are no mechanisms in place for verifying the accuracy, timeliness or completeness of PII. PII may be shared inadvertently during a ZoomGov session via discussion and/or application sharing. ZoomGov sessions may be recorded by the Host. The ZoomGov only records the audio, video and screen captures from the ZoomGov sessions.

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
IRS 10.004	Stakeholder Relationship Management and Subject 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.

Biometrics-In order for the ZoomGov application to be able to have video, the individuals participating in the ZoomGov sessions may opt to use their workstation camera to have a virtual face to face experience.

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?

No

When will the e-RA be completed?

12/31/2020

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 business units are responsible for notifications to individuals. The host of the ZoomGov session will have the ability to record the session. When the recording feature is initialized, all attendees of that ZoomGov session will receive an on-screen notification stating that the session is now being recorded. And those attending that session will then be given an option to remain in, or to leave the meeting.

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):

The individual can refuse to stay in a recorded session and leave the meeting.

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

ZoomGov provides IRS personnel a mechanism to conduct teleconferences and web conferences with personnel within the IRS WAN (Wide Area Network) and external participants via the Internet. As a result, the potential exists for sharing personally identifiable information (PII) and sensitive but unclassified (SBU) data. During the ZoomGov sessions and web conferences, hosts and participants may discuss PII and SBU data in support of the IRS mission so long as IRS employees and cleared contractors adhere to all IRMs governing discussion of PII and/or SBU.

INFORMATION PROTECTION

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

Contractor Owned and 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?

The ZoomGov recordings will be saved on the host's local workstation. The Host will have the ability to download detailed reports from his/her hosted session from the ZoomGov web portal. The reports are only available to those with a ZoomGov host license, which is approved through the OL5081 process. Access is secured via IRS PIV Card identification and authentication services. The PII data available for access in this application is required for their operation.

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?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

All records will be deleted or destroyed in accordance with approved retention periods. Any records will be managed according to requirements under IRM 1.15.1 and 1.15.6.14. Use of Collaboration Tools and will be destroyed using IRS General Records Schedule (GRS) or IRS Records Control Schedule (RCS) and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. Log files will be maintained in accordance with GRS 3.2, item 030, or 031.

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 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 for the Zoom Proof of Concept.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

Because this is a managed service in the cloud, we can only test our use cases. The results are in the ITUNSZoomGov share point folder.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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 testing included the testing of both Windows 7 and Windows 10. Tests also included ZoomGov features such as logging in, passwords, and features such as chat, breakout rooms, audio, video, outlook, and more. Bandwidth testing also took place and the results are located in the ZoomGov share point folder. Use case testing was done using different use case scenarios.

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: 50,000 to 100,000

Contractors: More than 10,000

Members of the Public: Under 100,000

Other: No

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?

No