U.S. Department of Justice

Privacy Impact Assessment
for
Zoom for Government

Issued by:
Katherine Harman-Stokes
Director (Acting)

Approved by: Katherine Harman-Stokes
Director (Acting)
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: 1/30/2023

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The U.S. Department of Justice ("Department," or "DOJ") is using Zoom Video Communications, LLC's FedRAMP authorized Zoom for Government Software-as-a-Service platform. The Department uses other collaboration platforms, which are documented separately; however, these platforms do not fully satisfy Department components' collaboration needs. The Department intends to bolster its components' internal and external communication abilities by providing a platform capable of effectively hosting large, virtual conferences. Zoom for Government unifies cloud video conferencing, simple online meetings, and a software-defined conference room solution into one platform, which offers video, audio, and wireless screen-sharing across multiple operating systems.

DOJ conducted this Privacy Impact Assessment (PIA) because the information collected, maintained, used, or disseminated by the system includes personally identifiable information (PII) about individuals, such as contact information, authorized voice recordings, and video images. Given the free flow of information during a video or voice conference, a potentially significant amount of personally identifiable information, including information related to civil or criminal litigation, may be shared through the use of Zoom for Government. This PIA is intended to encompass the use of the software by Department components in their ordinary course of business, and is not intended to cover any contractor-managed Zoom for Government subscription which might be used to fulfill component contracted services.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

In response to a changing work environment, the Department has increased its reliance on technology to bridge emerging communication and collaboration gaps. The Department has found large teleconferences are a critical form of communication and aid in a variety of workforce management areas. As described above, previously existing collaboration platforms do not fully satisfy Department components' collaboration needs. Specifically, Zoom for Government provides Department users with the ability to effectively host large teleconferences. Department users may also be able to use Zoom for Government to record meetings that they host, subject to component policies and the DOJ Policy Memorandum "Recording Department Meeting/Event Platforms," issued in February 2022.

The personal information required to establish a Zoom for Government account is minimal and mostly related to account management and licensing. Zoom for Government may also be used by Department components to conduct operational or other mission-related activities, such as interviews. Given the

varied nature of the Department's work and because meetings on Zoom for Government could conceivably implicate almost any element of personal information, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated during meetings on Zoom for Government. However, components are responsible for ensuring that their use of Zoom for Government falls within relevant authorities, law, and policy, and where such use extends beyond the scope of this document, for providing appropriate documentation as required by the eGovernment Act of 2002.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

	Authority	Citation/Reference
	Statute	• Federal laws that authorize the Attorney General to create and maintain federal records of agency activities, including but not limited to 5 U.S.C. § 301 and 44 U.S.C. § 3101 • Federal Records Act, 44 U.S.C. § 3301
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	• DOJ Electronic Messaging Records Retention Instruction 0801.04.02 • Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012 • Presidential Memorandum on Transparency and Open Government, January 21, 2009

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

Zoom for Government is an online collaboration tool that may appropriately implicate significant quantities and wide varieties of personal information. Given the varied nature of DOJ's work and because meetings on Zoom for Government could conceivably implicate almost any element of personal information, it is not possible to list with certainty every item

of information that will be collected, maintained, or disseminated during meetings on Zoom for Government.

Accordingly, the chart below reflects the information that is anticipated to be collected, maintained, or disseminated through DOJ users' registration for accounts and operation of the system itself.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name and business contact information	X	A, B, C, D	DOJ users are required to enter a name and email address to establish an account. Meeting participants may choose, but are not required to display their name during meetings. Meeting participants may choose to dial into meetings, displaying their business phone number.
Date of birth or age	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate dates of birth or ages. However, this information is not required to access Zoom for Government.
Place of birth	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate places of birth. However, this information is not required to access Zoom for Government.
Gender	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate gender. However, this information is not required to access Zoom for Government.
Race, ethnicity or citizenship	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate race, ethnicity, or citizenship. However, this information is not required to access Zoom for Government.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Religion	X	A, B. C. D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate religion. However, this information is not required to access Zoom for Government.
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate Social Security Numbers. However, this information is not required to access Zoom for Government.
Tax Identification Number (TIN)	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate Tax Identification Numbers. However, this information is not required to access Zoom for Government.
Driver's license	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate driver's license information. However, this information is not required to access Zoom for Government.
Alien registration number	X	C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate alien registration numbers. However, this information is not required to access Zoom for Government.
Passport number	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate passport numbers. However, this information is not required to access Zoom for Government.
Mother's maiden name	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate mothers' maiden names. However, this information is not required to access Zoom for Government.
Vehicle identifiers	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate vehicle identifiers. However, this information is not required to access Zoom for Government.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Personal mailing address	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate personal mailing addresses. However, this information is not required to access Zoom for Government.
Personal e-mail address	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate personal e-mail addresses. However, this information is not required to access Zoom for Government.
Personal phone number	X	A, B, C, D	Meeting participants may choose to dial into meetings, displaying their phone number.
Medical records number	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate medical records. However, this information is not required to access Zoom for Government.
Medical notes or other medical or health information	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate medical information. However, this information is not required to access Zoom for Government.
Financial account information	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate financial account information. However, this information is not required to access Zoom for Government.
Applicant information	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate account information. However, this information is not required to access Zoom for Government.
Education records	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate education records. However, this information is not required to access Zoom for Government.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Military status or other information	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate military information. However, this information is not required to access Zoom for Government.
Employment status, history, or similar information	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate employment information. However, this information is not required to access Zoom for Government.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate employee performance ratings. However, this information is not required to access Zoom for Government.
Certificates	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate certificates However, this information is not required to access Zoom for Government.
Legal documents	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate legal documents. However, this information is not required to access Zoom for Government.
Device identifiers, e.g., mobile devices	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate device identifiers. However, this information is not required to access Zoom for Government.
Web uniform resource locator(s)	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate URLs. However, this information is not required to access Zoom for Government.
Foreign activities	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate foreign activities. However, this information is not required to access Zoom for Government.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate criminal records information. However, this information is not required to access Zoom for Government.
Juvenile criminal records information	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate juvenile criminal records information. However, this information is not required to access Zoom for Government.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate civil law enforcement information. However, this information is not required to access Zoom for Government.
Whistleblower, e.g., tip, complaint or referral	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate whistleblower information. However, this information is not required to access Zoom for Government.
Grand jury information	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate grand jury information. However, this information is not required to access Zoom for Government.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate witness information. However, this information is not required to access Zoom for Government.
Procurement/contracting records	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate procurement information. However, this information is not required to access Zoom for Government.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Proprietary or business information	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate proprietary or business information. However, this information is not required to access Zoom for Government.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate location information. However, this information is not required to access Zoom for Government.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate photographs. However, this information is not required to access Zoom for Government.
- **Video containing biometric data**	X	A, B, C, D	Meeting participants may choose, or be required to display their video feeds.
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C, D	Meeting participants may choose, or be required to speak during meetings.
- **Scars, marks, tattoos**	X	A, B, C, D	Given the varied nature of DOJ's work, meetings on Zoom for Government will likely implicate scar, mark, or tattoo information. However, this information is not required to access Zoom for Government.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	DOJ users who create accounts are assigned user IDs.
- **User passwords/codes**	X	A	DOJ users who create accounts establish passwords.
- **IP address**	X	A, B, C, D	
- **Date/time of access**	X	A, B, C, D	

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Given the varied nature of DOJ's work and because meetings on Zoom for Government could conceivably implicate almost any element of personal information, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated during meetings on Zoom for Government.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	X
Phone	X	Email	X		
Other (specify): Minimal information is collected directly from DOJ users to establish Zoom for Government accounts. During meetings, information may be collected from DOJ users or meeting participants either online, or by telephone.					
Government sources:					
Within the Component	X	Other DOJ Components	X	Online	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): During meetings, information may be collected from DOJ users or meeting participants, which may include anyone that DOJ appropriately does business with or interacts with while conducting mission activities.					
Non-government sources:					

Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers	X				
Other (specify): During meetings, information may be collected from DOJ users or meeting participants, which may include anyone that DOJ appropriately does business with or interacts with while conducting mission activities.					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	DOJ users can access recordings for meetings that they hosted, which will be stored in the Zoom for Government platform via the online portal. Administrative access is required to view content created by other users. Further, meeting recordings may be shared with meeting participants or other component personnel for lawful and appropriate purposes.
DOJ Components	X			Meeting recordings may be shared with meeting participants or other DOJ personnel for lawful and appropriate purposes.
Federal entities	X			Meeting recordings may be shared with meeting participants or other federal personnel for lawful and appropriate purposes.
State, local, tribal gov't entities	X			Meeting recordings may be shared with meeting participants or other government personnel for lawful and appropriate purposes.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Public	X			Meeting recordings may be shared with meeting participants or other members of the public for lawful and appropriate purposes.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Meeting recordings may be shared with meeting participants or other counsel, parties, witnesses, and courts or tribunals for lawful and appropriate purposes.
Private sector	X			Meeting recordings may be shared with meeting participants or other private sector personnel for other lawful and appropriate purposes.
Foreign governments	X			Meeting recordings may be shared with meeting participants or other foreign government personnel for lawful and appropriate purposes.
Foreign entities	X			Meeting recordings may be shared with meeting participants or other foreign entities for lawful and appropriate purposes.
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

No information will be released from Zoom for Government for Open Data purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

Pursuant to Department policy, participants are given clear, advance notice if a meeting is being recorded prior to the start of the meeting, and meeting participants typically can control whether or not to share their video and audio.

DOJ also provides individuals with generalized notice about its collection, use, and sharing of PII through a variety of Systems of Records Notices (SORNs), and, in some instances, individualized notice pursuant to Section 552a(e)(3) of the Privacy Act of 1974. The types of information potentially collected, used, and shared through the use of Zoom for Government are covered under several applicable DOJ SORNs, including those listed in Section 7.2 of this PIA. A full list of DOJ SORNs is available online at www.justice.gov/opcl/doj-systems-records.

Further, where information is collected into, maintained as part of, or used or disseminated from a DOJ System of Records, such collection, use, maintenance, and dissemination will be conducted in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a and consistent with each relevant SORN.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

DOJ users who register for Zoom for Government accounts are required to provide basic contact information in order to use the platform. Meeting participants who sign into a meeting on Zoom for Government online have the option to modify their display name to preclude identification, and typically can control whether or not to share their video and audio.

In accordance with DOJ policy, participants are notified whenever a meeting is being recorded. In most circumstances, participants may decline to participate in the meeting or recording.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Freedom of Information Act (FOIA) or Privacy Act requests may be submitted to components by following these instructions: https://www.justice.gov/oip/make-foia-request-doj. Within DOJ, each component processes its own records in response to FOIA requests. Therefore, each request will receive the quickest possible response if it is addressed directly to the component which holds the relevant records.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

	The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO): **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**
X	The DOJ ATO for Zoom for Government was initially approved on February 11, 2021, and will remain active until January 20, 2023.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Security control assessments for Zoom for Government, and for the Cloud Service Provider, are conducted on a routine basis as required by NIST, FedRAMP, and DOJ policy requirements. At DOJ, assigned Information System Security Officers (ISSOs) ensure that appropriate security controls are in place and relevant information is uploaded into the Cyber Security Assessment and Management (CSAM) System, the Department's system inventory application. Zoom for Government has been authorized at the FedRAMP Moderate Level and is reviewed at least annually, which is the current requirement for a FISMA system that has been designated as "moderate" under Federal Information Processing Standards (FIPS) Publication 199.[1] Component information technology teams will ensure that necessary cybersecurity controls are in place and that FISMA and FedRAMP compliance
X	documentation is completed before the use of Zoom for Government at DOJ.
	Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted: Zoom for Government follows the Audit and Accountability (AU) controls outlined by NIST 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations.[2] Auditing provides visibility into important security events via log files and suspicious events are forwarded to the Department's iteration of Splunk for correlation, reporting, and archiving on a regular basis.[3] Zoom for Government audit and accountability procedures are
X	reviewed annually, and audit and accountability policies are reviewed every three years.

[1] See https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.
[2] See https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
[3] The Department's iteration of Splunk captures, indexes, and correlates "real-time" event data in a searchable repository

X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe: Prior to accessing Zoom for Government, and subsequently on an annual basis, DOJ users with a Zoom for Government account must complete applicable DOJ or component Cybersecurity Awareness Training, and both review and agree to comply with the DOJ or component IT Rules of Behavior.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

Zoom for Government has a security categorization of FISMA moderate as described in NIST Special Publication (SP) 800-60, Vol. II.[4] As a result, Zoom Video Communications, LLC, has assessed and implemented applicable security controls to ensure protections commensurate with the impact to the Department from unauthorized access or disclosure of information.

Zoom for Government provides a range of physical and technical safeguards to prevent unauthorized access to the platform, including transport layer security encryption,[5] 256-bit encryption,[6] role-based user security, firewall compatibility, and a password-protected meeting option.

Further, privacy controls may be made available through the DOJ Common Control Program. Common controls are security and privacy controls that are implemented centrally, but can be inherited amongst many systems. During the control selection process, system owners inherit controls provided by a common control provider as long as the control is applicable to their information system and meets the unique system requirements.

---

from which IT and information security staff can generate graphs, reports, alerts, dashboards, and visualizations of various events. Splunk provides insight into operational, security, and functional aspects of the environment, and is covered under separate privacy documentation.

[4] See https://csrc.nist.gov/publications/detail/sp/800-60/vol-2-rev-1/final.

[5] Transport layer security (TLS) is a protocol that provides communication security between client/server applications that communicate with each other over the Internet. (www.techopedia.com)

[6] 256-bit encryption is a data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files. (www.techopedia.com)

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

In accordance with National Archives and Records Administration (NARA) Bulletin 2010-05, Guidance on Managing Records in Cloud Computing Environments, Zoom for Government must ensure that federal records stored on its cloud-based environment are readable and accessible throughout their respective life cycle.

Information collected and maintained by the Department is retained and disposed of in accordance with the General Records Schedule retention schedule applicable to the component, information, and context of the information's collection or maintenance.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

- JUSTICE/DOJ-002 Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full 86 Fed. Reg. 1352 (Jul. 14, 2021).

- JUSTICE/DOJ-003 Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (Jun. 4, 2001), 66 Fed. Reg. 34743 (Jun. 29, 2001), 67 Fed. Reg. 65598 (Oct. 25, 2002), and 82 Fed. Reg. 24147 (May 25, 2017).

- JUSTICE/DOJ-014, Department of Justice Employee Directory Systems, last published in full at 74 Fed. Reg. 57194 (Nov. 4, 2009) and modified at 82 Fed. Reg. 24151, 153 (May 25, 2017).

Given the varied nature of DOJ's work and because meetings on Zoom for Government could conceivably implicate records in multiple DOJ Systems of Record, it is not possible to list with certainty every System of Records Notice (SORN) into which information will be collected, or from which information may be disseminated during meetings on Zoom for Government. However, records that are collected into, or disclosed from DOJ SORNs will be collected, maintained, used, and disseminated in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, and the applicable SORN(s).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

The primary privacy risk associated with the Department's use of Zoom for Government is the potential for unauthorized access to, and subsequent misuse of PII. Department users and meeting participants may share PII about themselves or others during virtual meetings, whether verbally, through chat or direct messaging, or while sharing their video, audio, or other information on their screens or their applications. To mitigate the risk of unauthorized access to, or subsequent misuse of PII, Department users may limit attendance to a particular meeting to individuals who have authorization to access the information to be discussed, may provide notices or announcements recommending that participants limit their disclosure of extraneous PII, or may limit the features available during the meeting, for example by turning off the chat function, refusing screen sharing requests, and muting participants and turning off their video sharing as needed to limit attendee participation.

Information may also be disclosed to individuals without authorized access, and who may misuse the information, through the sharing of recordings; accordingly, DOJ has taken efforts to limit recordings. The issuance of DOJ Policy Memorandum, *Recording Department Meeting/Event Platforms*, in February of 2022 established Department-wide policy for the use and maintenance of content captured, created, or shared using recording capabilities in Zoom for Government.[7] The policy specifically states that the recording capability must only be used in limited circumstances, where the recording is necessary and permitted by law. Recordings should not be used to replace traditional meeting minutes or notes, and components should establish written component-level policy that identifies appropriate uses for recording capabilities based on component mission and function requirements. The Policy states that recordings must not remain on individual drives, such as OneDrive, but rather, should be moved to the appropriate recordkeeping repository. The Zoom for Government host who made the recording must ensure the safe storage and handling of any recordings with sensitive information, and a recording may be shared with non-

[7] DOJ recordkeeping policies follow 44 U.S.C. §§ 3101 *et seq;* 5 U.S.C. § 301and DOJ Order 0801 Records and Information Management.

participants only after analyzing the associated privacy risks, including whether PII has been protected appropriately and whether sufficient notice was provided to the participants in the recording. In the event that a recorded training is shared for later viewing, the sharing process should minimize the duplication of the files so that viewing permissions are provided for the file rather than transmitting a copy of the file.

Separately, the risk of collecting erroneous or inaccurate information from individuals in the sign-in process is mitigated by only collecting the information necessary to conduct a Zoom for Government meeting. As noted above, Zoom for Government is not designated as an official record-keeping system for substantive information. Substantive information is to be moved to the appropriate recordkeeping repository and retained within the Department and disposed of by the components themselves, in accordance with the schedule applicable to such information.

According to Zoom for Government's data retention plan, information collected from DOJ users will be kept as long as the user maintains an active subscription. Users whose accounts are terminated will immediately lose access to Zoom for Government, but their name and user ID are maintained for ninety days from date of termination. Billing information may be maintained for seven years.