Federal Bureau of Prisons

Privacy Impact Assessment
for the
BOP Enterprise Web Conferencing Services (BOP-EWCS)

Issued by:

Michael Rogers
RIM Chief / SCOP

Approved by: Andrew J. McFarland
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: June 15, 2026

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or 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 Federal Bureau of Prisons (FBOP) Enterprise Web Conferencing Systems (BOP-EWCS) utilizes Video Conferencing system (VTC) and Webex to host events and meetings for FBOP employees, inmates, and members of the public. These systems provide video conferencing and meeting capabilities via authorized virtual collaboration in lieu of meeting in-person. This could include internal FBOP meetings, training, and hearings or meetings with criminal or immigration court officials or probation/parole officers for official proceedings. When specifically approved, authorized FBOP users may record a video conference (only applicable to FBOP-hosted meetings). Users may connect to the VTC and Webex online or by telephone. FBOP uses the FedRAMP authorized Cisco's Webex for the U.S. Government platform.

The FBOP conducted this Privacy Impact Assessment (PIA) because the information collected, maintained, used, or disseminated by the systems includes personally identifiable information (PII) about individuals, such as contact information (emails, phone numbers, names), and video images and voice, which may be recorded when specifically authorized. However, since VTC and Webex are hosted by Cisco, the FBOP does not maintain this data, except FBOP users who are authorized to maintain recordings. While only FBOP personnel, including employees, contractors and other individuals (interns and detailees) assigned to the FBOP, may schedule meetings/conferences using BOP-EWCS, the systems may capture information about other individuals who attend FBOP meetings/conferences, including other federal employees or members of the public on the BOP-EWCS platform. Given the free flow of conversation and information that may occur during a video or voice conference, there is the potential that a significant amount of personally identifiable information, including information related to civil and criminal litigation, may be shared through the use of BOP-EWCS. This PIA is intended to encompass the use of BOP-EWCS by the FBOP in the ordinary course of business.

Appendix A to this PIA lists and briefly summarizes the systems and applications that comprise the "Enterprise Web Conferencing Systems" under the control of the FBOP. Any additional conferencing/meeting systems procured at a future date will be addressed in their own initial privacy assessments and added to the Appendix.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), 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.

The FBOP has the responsibility of facilitating a reliable, secure way to host video and voice conference events and meetings to increase productivity, efficiency, and reduce travel expenses. The Webex platform enables FBOP employees (also referred to as "hosts") to coordinate and conduct meetings and attend conferences or trainings virtually from a desktop, laptop, or mobile device, as permitted, rather than in-person. The BOP-EWCS is intended to provide a stable digital conferencing platform for moderate to large group meetings utilizing Webex and the VTC systems provided by Cisco. Such meetings include the facilitation of meetings for inter-office or national training events, affirmative employment seminars, and inmate communications (judicial proceedings, immigration or parole hearings, attorney/client meetings, telehealth consults, reentry planning with U.S. Probation Offices, etc.).

Users include internal FBOP employees, other federal government users, as well as state, tribal, or local government users, or members of the public (to include inmates housed in federal custody). To administer these systems, the FBOP relies on role-based access. Users are assigned a role as either (1) administrator, (2) host, or (3) attendee. These roles can be further subdivided using various permissions, as deemed appropriate within the FBOP or for a specific meeting's needs. Administrators may also perform some basic trouble-shooting duties, such as resetting passwords and escalating troubleshooting issues to Cisco. FBOP users who are given permission to schedule meetings and invite attendees may serve as hosts. Attendees may include DOJ employees, approved DOJ contractors and external attendees, including members of the public and inmates (attendees are also referred to as "guests").

When a host establishes a meeting and invites attendees, an invitation e-mail is sent to attendees, which contains a link to the meeting and a password, which is required to access the meeting if enabled by the host. Attendees will be able to access the meeting from any device with internet access or by dialing a designated dial-in telephone number.

BOP-EWCS systems do not automatically record, store, or collect information in meetings; instead, the FBOP host must select the option to record the meeting (if pre-approved by the FBOP Director or their designee). Notice to attendees will automatically be provided if a meeting will be recorded. Absent prior authorization and notice to all participants, a meeting will not be recorded.

A host can activate the whiteboard feature during a meeting. The information from the whiteboard feature can vary depending on the specific meeting conversation and presentation. Information on the whiteboard does not save on Webex after the meeting ends. Webex does not maintain any copies of the collaborative content. Recordings are maintained in the system until downloaded.

For FBOP users authorized to record meetings, the host must save the recording on their FBOP equipment or system (desktop, shared FBOP office folder, etc.) following the meeting or it will be erased from FBOP's cloud environment system after 60 days. Cisco does not maintain any copies of the recordings or collaborative content (content shared during the recorded meeting). Cisco manages the systems, and as a result collects and maintains log data. Cisco generates statistical reports that may be stored by the FBOP administrators for no longer than 90 days. Cisco may log attendees' names, contact information including email addresses or telephone numbers, if used, and user roles as required to facilitate meetings and issue meeting invitations. Cisco regularly provides the FBOP with usage and trending reports which do not contain PII.

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	• 18 U.S.C. §§ 3621, 4042 (federal inmates), 5003 (state inmates) and Section 11201 of Pub. L. 105-33; 111 Stat. 740 (DC Offenders); 44 U.S.C. §§ 3101 and 3301 • 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	• 28 CFR part 540
Agreement, memorandum of understanding, or other documented arrangement	• DOJ Policy Memorandum, *Recording Department Meeting/Event Platforms*, in February of 2022
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 • 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.

While Cisco offers a comprehensive suite of features for users, the FBOP only uses the functions needed to conduct virtual meetings, events and training. The table below depicts both the possible data that may be captured by the FBOP during the use of the systems and the types of data Cisco collects on behalf of the FBOP. Due to the varied nature of the FBOP's work, recordings of video or voice conferences could potentially include almost any type of unclassified PII. It is not possible to list with certainty every type of information that may be collected, maintained, or disseminated by the FBOP through the use of the systems.

(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	X	A, B, C and D	Names and usernames of site administrators, hosts, and attendees, which may include members of the public and inmates.
Date of birth or age			
Place of birth			
Sex			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			

(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 and D	Mailing addresses may be added by the user into their profile to confirm their identity and ensure an inmate is not meeting with a co-conspirator or for other criminal and legal purposes.
Personal e-mail address	X	A, B, C and D	Emails are used by hosts to invite attendees, which then allows guests to attend the BOP-EWCS. Emails may also be added by the user into their profile to confirm their identity and ensure an inmate is not meeting with a co-conspirator or for other criminal and legal purposes.
Personal phone number	X	A, B, C and D	An attendee may join the conference using their personal phone and their phone number will be displayed in the meeting. Personal phone numbers may also be added by the user to their profile to confirm their identity and ensure an inmate is not meeting with a co-conspirator or for other criminal and legal purposes.
Medical records number			
Medical notes or other medical or health information	X	A, B, C and D	May include inmate name and medical test procedure or diagnosis as the conference name (with employees or contractors).
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			

(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
Device identifiers, e.g., mobile devices	X	A, B, C and D	Cisco collects host and attendee device identifiers, IP addresses, and browser type (whether the user accessed the meeting through a mobile app or web-based browser). Cisco's data analytics can only determine which users are FBOP users versus guests. It cannot trace the IP address to a specific individual.
Web uniform resource locator(s)	X	A, B, C, and D	Cisco collects unique meeting URLs linked to the meeting ID and user when creating an IT Service Desk ticket for service.
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information	X	A, B, C and D	Emails and phone numbers may be added by the user to their profile but is not a requirement.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C and D	IP addresses can provide a city and state location for an individual calling into Webex.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C and D	Hosts may upload photographs for their user profiles, but it is not a requirement.
- **Video containing biometric data**	X	A, B, C and D	Video transmission and recordings include biometric data within the video transmission and may be included in the video recording.

(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
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C and D	Voice signatures are transmitted during a meeting and voice recordings are collected when the meeting is recorded.
- **Scars, marks, tattoos**	X	A, B, C and D	A user's scar, mark, or tattoo may be transmitted or recorded if the user's camera is on during the meeting.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A	Both Cisco and FBOP capture a record of the authorized users with administrative capabilities.
- **User ID**	X	A, B, C and D	Cisco collects this information.
- **User passwords/codes**	X	A, B, C and D	Cisco collects this information.
- **IP address**	X	A, B, C and D	Cisco collects this information.
- **Date/time of access**	X	A, B, C and D	Cisco collects this information.
- **Queries run**	X	A	Cisco collects this information.
- **Contents of files**	X	A, B, C and D	FBOP may retain video recordings and other collaborative content, if approved.
Other (please list the type of info and describe as completely as possible):	X	A, B, C and D	The recording metadata collected could include meeting/event date, time subject, names of all attendees, case project file name/number (if appropriate), recording save location (url or file path, if appropriate). The PII identified in the Chart above is the most certain and foreseeable use of PII in the systems; however, since meetings can be recorded it is possible that other PII elements in this Chart that are not selected, as well as PII elements not identified in this Chart, can also be collected in the recording of the meeting.

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

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax		Online	X
Phone	X	Email	X		
Other (specify): Information may be received from a user via smart tablet, computer, smartphone or telephone.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	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): FBOP can meet with the categories of sources provided above, therefore, these sources may produce information during the meeting. Specifically, information may be collected from foreign governments on treaty transfer, hearings, and/or trial meetings on inmates.					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	X
Commercial data brokers					
Other (specify):					

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			Information collected by FBOP, primarily recordings, will only be shared on a case-by-case basis as needed.

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.**
DOJ Components	X			Information collected by FBOP, primarily recordings, will only be shared on a case-by-case basis as needed.
Federal entities	X			Information collected by FBOP, primarily recordings, will only be shared on a case-by-case basis as needed.
State, local, tribal gov't entities	X			Information collected by FBOP, primarily recordings, will only be shared on a case-by-case basis as needed.
Public	X			Information collected by FBOP will only be shared on a case-by-case basis as needed and as authorized by FBOP Office of the General Counsel.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Information collected by FBOP, primarily recordings, will only be shared on a case-by-case basis as needed and as authorized by FBOP Office of the General Counsel.
Private sector	X			Information collected by FBOP, primarily recordings, will only be shared on a case-by-case basis as needed and as authorized by FBOP Office of the General Counsel.
Foreign governments	X			Information collected by FBOP, primarily recordings, will only be shared on a case-by-case basis as needed and as authorized by FBOP Office of the General Counsel.

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.**
Foreign entities	X			Information collected by FBOP, primarily recordings, will only be shared on a case-by-case basis as needed and as authorized by FBOP Office of the General Counsel.
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 for Open Data purposes.

Section 5: Notice, Consent, Access, and Amendment

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

FBOP provides individuals with generalized notice about its collection, use, and sharing of PII through a variety of Systems of Records Notices (SORNS), including:

- Individuals have been notified that account information, audit logs, and user records maintained by the FBOP to plan and manage system services are covered under JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full 86 Fed. Reg. 1352 (July 14, 2021).

- Webex information such as shared/sent meeting invitations are covered by JUSTICE/DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (June 4, 2001), 66 Fed. Reg. 34743 (June 29, 2001), 67 Fed. Reg. 65598 (Oct. 25, 2002), and 82 Fed. Reg. 24147 (May 25, 2017).

- DOJ employee records maintained in this system are covered by 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).

For meetings that will be recorded, participants are given explicit notice prior to the start of the meeting that the event will be recorded.

In addition to the limited information that may be collected, used, and/or shared by the FBOP, Cisco collects the information that users provide, in accordance with their terms of service and privacy policies. A disclaimer stating, "By logging into Webex, you agree to the terms of this notice and the Cisco agreement referenced. If you are acting on behalf of a company or other legal entity, you represent that you have the authority to bind such entity and its affiliates, in which case "you" or "your" shall refer to such entity and its affiliates. If you do not have such authority, or if you do not agree with the above notice or the Cisco agreement, do not use Webex."

Links are provided for:

- Terms of Service - https://www.cisco.com/site/us/en/about/legal/contract-experience/index.html;
- Privacy Statement - https://www.cisco.com/c/en/us/about/legal/privacy.html; and
- Notices & Disclaimers - https://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html.

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.

Individuals outside of the FBOP must provide their name and email address or phone number to participate in meetings. For individuals within the FBOP, the information technology section creates user profiles based on information pulled from the Active Directory such as name and work email address. Opportunities exist for internal and external FBOP users to provide additional information to associate with their profile when signing up for an account, but it is not required.

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.

All users may access or amend their profile data at any time. Access or amendment requests for user records that are maintained by the FBOP can be requested in accordance with JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," last published in full at 86 Fed. Reg. 1352 (Jul. 14, 2021). Recordings of meetings document what occurred in the video conference, e.g.,

what was said by whom, cannot be amended to ensure accuracy and a proper account of the meeting.

Individuals seeking to gain further access to information that is maintained by DOJ within Cisco may request amendment or correction of their respective information by making a FOIA and/or Privacy Act request by following the provisions of those statutes and DOJ regulations on those statutes. Further instructions on how to submit a request are provided at Part 16 of Title 28 of the Code of Federal Regulations.

Cisco has detailed the procedures for individuals to request access, rectification, suspension of processing or deletion of personal data in the Privacy Data Sheet, available at https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/cisco-webex-meetings-privacy-data-sheet.html#11Howtoexerciseyourdatasubjectrights.

Section 6: Maintenance of Privacy and Security Controls

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

X	**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 the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** The ATO for the BOP-EWCS was authorized on 5/14/2026 and expires on 5/14/2029. **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:**
	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:
	This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification,

	which may be detailed in the system security and privacy plan: BOP-EWCS maintains any type of criminal incarceration/rehabilitation, legal, or health information may be discussed or recorded during meetings. If a loss of availability, integrity, or confidentiality regarding this information were to occur, the worst-case scenario would be that individuals may suffer an adverse impact from a breach of confidentiality of their personal information, and/or the FBOP may suffer an adverse effect on public and inmate confidence. Under NIST SP800-60 Volume 2, Rev 1, this information properly falls under Federal Correctional Activities, Health, Litigation and Judicial Activities, with default categorization of High, and special factors listed that could result in higher or lower impact level. The special factors listed are: None. Based on the specific facts of this scenario, there are no mitigating or aggravating factors, special factors are not implicated because the information types that may be held within BOP-EWCS already result in a high impact level.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Cisco manages and maintains compliance of configuration changes required for maintenance, vulnerability management, and all continuous monitoring aspects of the system. They will also perform configuration changes to improve the security posture when necessary. Configuration changes include updating vendor products, updating configuration baselines to remediate vulnerabilities, applying all security patches, and editing continuous monitoring profiles to increase auditing capabilities.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** BOP-EWCS follows the Audit and Accountability (AU) controls by NIST 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. Auditing provides visibility into important security events via log files and suspicious events are forwarded to the FBOP for correlation, reporting, and archiving on at least a quarterly basis. Audit and accountability procedures are reviewed annually, and audit and accountability policies are reviewed every three years.
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** Contractors are responsible for complying with the applicable policies and procedures in accordance with the security posture established by Cisco senior management and with applicable contracts with the FBOP, as documented in their Statement of Work and other procurement documentation. Cisco requires basic security awareness training for employees and contractors that support the operation of the contractor systems. Those who have additional access will have information security technical training to understand their information system security roles.
X	**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: No additional training is necessary for users. However, prior to accessing the BOP-EWCS, and subsequently on an annual basis, all internal FBOP users must complete computer security awareness training, as well as review and agree to comply with DOJ's Rules of Behavior. System administrators will complete additional professional training, including security training and the Role-Based IT Professional Training-Security Awareness for assigned administrators.

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?

The following access and security controls have been utilized to protect privacy by reducing the risk of unauthorized access and disclosure:

- BOP-EWCS has a security categorization of FISMA moderate as described in NIST Special Publication 800-53. FBOP uses the FedRAMP-authorized government version. As a result, the FBOP information technology section has assessed and implemented applicable security controls to ensure protections commensurate with the impact of the FBOP from unauthorized access or disclosure of information.
- BOP-EWCS restricts access to log data only to users designated as system administrators with a specific need to review that data. Only systems administrators are granted access to search and retrieve the meeting data within the FBOP. Host users may only access their own account and meeting data. Attendees have an even more limited role with BOP-EWCS because they do not have access to the data beyond their individual profile within the meeting.
- BOP-EWCS is protected by multiple firewalls, an intrusion prevention system, real-time continuous monitoring using malicious code detection and protection, encryption, and other technical controls in accordance with applicable security standards.
- It is made clear to users, through visual indicators, when a meeting contains participants that are not part of the FBOP. Meetings can be moderated such that moderators have exclusive control of the room's participants.
- All passwords and user-generated information are encrypted at rest and in-transit. Web-based information transmitted between FBOP and Cisco during meetings are encrypted using the highest level of encryption supported, consistent with applicable NIST standards.
- Data collected from meetings are stored for ninety days for Cisco to run back-end performance reports.

- For FBOP users authorized to record meetings, the host must save the recording on their FBOP equipment or system (desktop, shared FBOP office folder, etc.) following the meeting or it will be erased from Webex's cloud environment after 60 days. Cisco does not retain copies of recorded meetings. Recordings are only permitted for hosts who have received prior authorization by the FBOP Director or his/her designee.

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.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.

Cisco maintains data collected for the purpose of providing back-end analytics to the FBOP for ninety days. Meeting recordings are maintained in Webex's cloud environment system for 60 days, after which they are deleted unless the recordings are downloaded by FBOP staff. System access records are maintained for 6 years after the password is altered or the user account is terminated.

Information downloaded and stored within the FBOP, such as meeting recordings, is to be retained, and disposed of in accordance with the General Records Schedule or FBOP retention schedule applicable to such information.

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, 86 Fed. Reg. 1352 (July 14, 2021), available at https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf.
- JUSTICE/DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (June 4, 2001), 66 Fed. Reg. 34743 (June 29, 2001), 67 Fed. Reg. 65598 (Oct. 25, 2002), and 82 Fed. Reg. 24147 (May 25, 2017), available at https://www.gpo.gov/fdsys/pkg/FR-2001-06-04/pdf/01-13860.pdf.

- 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), available at https://www.gpo.gov/fdsys/pkg/FR-2009-11-04/pdf/E9-26526.pdf.
- Justice/BOP-005, BOP's Inmate Central Records System, published at 48 FR 23711 (June 7, 1984) and last modified at 84 FR 19809 (May 16, 2019) and available at https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf
- Justice/BOP-007, BOP's Inmate Physical and Mental Health Record System, 82 FR 49906 (June 12, 2024), available at https://www.govinfo.gov/content/pkg/FR-2024-06-12/pdf/2024-12221.pdf.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the FBOP 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? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

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,***
- ***Type of technology employed (e.g. AI/ML),***
- ***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 risks associated with the FBOP's use of BOP-EWCS are overcollection of information, maintenance of inaccurate information, unauthorized access, or misuse of PII.

Individuals who interact (participate in meetings, share their screen, post comments in meeting chat, etc.) with the FBOP using BOP-EWCS may submit additional information to the FBOP when participating in virtual meetings. These interactions may expose the FBOP to the user's PII. To mitigate this risk, the FBOP host may limit the capabilities available during the meeting, such as turning off the comment function or limiting occasions during which attendees may speak freely. Further, the host acts as the gatekeeper for those authorized to attend. Meeting invites sent by FBOP hosts are directed to specific individuals.

During meetings, users outside of the FBOP may participate as attendees. Both groups of users (internal to FBOP and outside of FBOP) have same user capabilities: attend meetings, change their username, and raise their hand. The host(s) have more control during a meeting. They can record a meeting, if authorized, share documents which may be downloaded by attendees, override all volume controls, enable waiting rooms, lock meetings, and enable passwords for their meetings for access control purposes. Despite the FBOP assigned user roles that impact user functions, users can also take screenshots of the meeting at any time via their own device.

FBOP has taken additional efforts to limit recordings, and therefore, the overcollection of information. The issuance of DOJ Policy Memorandum, *Recording Department Meeting/Event Platforms*, in February of 2022 established DOJ policy for the use and maintenance of content captured, created, or shared using recording capabilities in BOP-EWCS. The policy specifically states that the recording capability must only be used in limited circumstances where recording is necessary and permitted by law. Recordings should not be used to replace traditional meeting minutes or notes. The Memorandum states that recordings must not remain on individual drives, such as OneDrive, but rather, should be moved to the appropriate recordkeeping repository as necessary. The host who made the recording must ensure the safe storage and handling of any recordings with sensitive information. A recording may be shared with non-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.

Next, the risk of collecting erroneous or inaccurate information from individuals is mitigated by only collecting what is necessary. While Cisco may offer facial recognition features, capabilities for an automated assistant to hold simultaneous rooms and meetings, some level of artificial intelligence to provide a more personalized user experience for other clients, FBOP's usage of Cisco does not include these additional features. BOP-EWCS is not designated as an official record-keeping system for substantive information. Substantive information is to be retained within the FBOP and disposed of in accordance with the retention schedule applicable to such information.

Additionally, to ensure accurate information about users, users have access to their own profile and may correct that information at any time. However, recordings of meetings are unable to be altered.

To mitigate the risk of unauthorized access or disclosure of FBOP information, BOP-EWCS does not connect to any other FBOP major or minor system. FBOP information technology employees verify BOP-EWCS users against the DOJ's Active Directory and the user must then be admitted to the FBOP network before the user is eligible to access or use BOP-EWCS on their authorized work web and mobile devices.

Additionally, Cisco implements a variety of privacy mitigation strategies to prevent unauthorized access of information, which includes not selling personal data, not tracking user usage data for advertising purposes, and not interfering with meeting traffic or content. Cisco offers technical

security measures to users such as encrypting data at rest and in transit. In the event of a breach, Cisco's Security and Trust Organization coordinates the Data Incident Response Process on an enterprise-wide level by having a breach and incident notification process in place. For users whose accounts are terminated, they immediately lose access to BOP-EWCS, but their name and user ID are maintained for ninety days from date of termination. Cisco maintains hosts usage information for ninety days while billing information may be maintained for seven years. FBOP maintains user data for no more than ninety days as set by the authorized FBOP administrators.

To mitigate the risk of users misusing PII, FBOP users are subject to the DOJ Rules of Behavior and receive annual cybersecurity and privacy training to notify them of their responsibilities when handling DOJ information and PII. Additionally, Cisco provides online resources for users to mitigate the misuse of PII on their platform. Cisco's Help Center provides best practices for hosts with tips for scheduling meetings, security during meetings, and suggestions to either delete or password protect recordings stored by the FBOP post-meeting. Additionally, Cisco provides best practices for site administrators and their use of the meeting control hub, where administrators have the ability to manage the number of active users, the number of licenses and run statistical analysis reports.

APPENDIX A: FBOP

This Appendix lists the systems and applications collectively referred to as the "Bureau of Prisons Enterprise Web Conferencing Services (BOP-EWCS)" throughout this PIA. For each of these systems and applications, FBOP users authorized to record meetings, the host must save the recording on their FBOP equipment or system (desktop, shared FBOP office folder, etc.) following the meeting or it will be erased from Webex's cloud environment system after 60 days. Cisco does not retain copies of recorded meetings. Recordings are only permitted for hosts who have received prior authorization by the FBOP Director or his/her designee.

1. **Webex** – FBOP has the responsibility of facilitating a reliable, secure way to host video and voice conference events to increase productivity, efficiency, and reduce travel expenses. Cisco's Webex enables the FBOP to conduct meetings and attend conferences or trainings virtually, rather than in-person. Webex is intended to provide a stable digital conferencing platform for moderate to large group meetings. Such meetings include the facilitation of inmate communications (judicial proceedings, immigration or parole hearings, telehealth consults, reentry planning with U.S. Probation Offices, etc.). FBOP employees wishing to host a Webex meeting must access Webex using their government-issued laptop or mobile device. Invited attendees will be able to access the meeting from any device by unique meeting link or by dialing a designated dial-in telephone number generated by Webex. Webex provides the option to record a meeting; however, pursuant to DOJ policy, recordings are only permitted if prior authorization has been obtained. FBOP policy requires that requests to record Webex meetings must be approved by the FBOP Director or their designee. If the FBOP Director or their designee approves a recording request, Webex automatically provides notice to attendees if a Webex meeting will be recorded. A red circle is shown on the user's web interface that a meeting is being recorded. Users connecting to a meeting via dial-in will receive an automated message alerting them that the meeting is being recorded before they are allowed into the meeting room. Absent prior authorization and notice to all participants, a meeting will not be recorded. If recordings are authorized by the FBOP Director or their designee and activated by the host, the host may download the collaborative content at the conclusion of the meeting to their computer. Information held in the system may contain names/usernames, user profile information (if provided), device information, and voice/facial signatures (during recordings), as described in the PII section above. However, since meetings can be recorded it is possible that other PII elements can also be collected in the recording of the meeting.

2. **Video Conferencing System (VTC)** – The Video Conferencing (VTC) system enables the FBOP to carry out various official duties via virtual collaboration in lieu of meeting in-person. Such meetings include the facilitation of inmate communications (judicial, immigration or parole hearings, telehealth consults, reentry planning with U.S. Probation Offices, meetings with consular offices, etc.) and administrative staff meetings or training (inter-office or national training events, affirmative employment seminars, routine staff meetings, etc.). The VTC system is intended to provide a stable digital conferencing platform for moderate to large group meetings. The VTC system enables the FBOP to

conduct meetings and attend conferences or training from any registered VTC device. FBOP users can add non-FBOP participants by adding their email address or phone number to a scheduled VTC meeting or training session. Non-FBOP participants can only use the audio features when calling in. Information held in the system may contain names/usernames, user profile information (if provided), device information, and voice/facial signatures as described in the PII section above.