Court Services and Offender Supervision Agency (CSOSA)

Office 365
Privacy Impact Assessment

CONTROLLED UNCLASSIFIED INFORMATION

October 19, 2021

Office 365/Office of Information Technology
Court Services and Offender Supervision Agency
633 Indiana Avenue, NW, Washington, DC 20004

POINTS OF CONTACT for Office 0365

Program Office Point of Contact: **Name: Jennifer Epps** **Title: Deputy CIO** **Office: Information Technology** **Phone: 202 220-5452** **Bldg./Room: 800 North Capitol** **Email: Jennifer.epps@csosa.gov**	**System Owner Point of Contact** **Name: William Kirkendale** **Title: CIO** **Office: Information Technology** **Phone: 202 220-5300** **Bldg./Room** **Email: William.kirkendale@csosa.gov**
Privacy Program Manager: **Name:** **Office:** **Phone:** **Bldg./Room** **Email:**	**Senior Agency Official for Privacy:** **Name: Sheila Stokes** **Office: General Counsel** **Phone: 202 220-5797** **Bldg./Room** **Email: Sheila.stokes@csosa.gov**

THIS PAGE IS FOR INTERNAL ROUTING PURPOSES AND DOCUMENTATION OF APPROVALS. UPON FINAL APPROVAL, COMPONENTS SHOULD REMOVE THIS PAGE PRIOR TO PUBLICATION OF THE PIA.

Overview of Office 365

O365 will provide a new email, messaging, and collaboration solution to replace the existing CSOSA messaging and collaboration system. This system is comprised of the O365 product suite. O365 is a cloud SaaS computing-based subscription service offering from Microsoft that provides dedicated enterprise email and collaboration software. O365 provides customers with cloud versions of Exchange Online (EXO) and TEAMS.

The purpose of this Privacy Impact Assessment is to address the privacy risks associated with O365 use of Personally Identifiable Information (PII).

1. Description of the System

1.1. Describe the system, including the system name, system, acronym, and a brief description of the major functions.

O365 is a cloud-based Service (SaaS) solution that provides enterprise business productivity services and software. Licensed users have access to the services and software available via Office application integration. O365 includes services such as SharePoint Online, Dynamics Online, Power BI, Azure Information Protection, Skype for Business web conferencing, Exchange Online hosted e-mail for business, and additional online storage with OneDrive for Business. O365 includes the desktop version of the latest Office applications, which provide users a consistent experience across multiple computers and devices. These applications include Word, Excel, PowerPoint, OneNote, Outlook, Publisher, and forms to collected vaccine and medical data as required.

1.2. Describe the purpose for which the personally identifiable information (PII) is collected, used, maintained, or shared.

There are a variety of services and software available via Office application integration, used in the course of user's official business duties, and therefore all purposes cannot be anticipated or enumerated. A few examples include:

Exchange Online E-mail uses names and e-mail addresses and sends, with the potential to collect in users' mailboxes, other subject matter that could contain other examples of PII. For instance, Human Resources may retrieve SSNs and other personal information through disseminated attachments; CSOSA security office may request badge ID numbers from new hires; also temporary passwords (PINS) may be transmitted through the system. These are examples of how the O365 email system could be used.

SharePoint Online serves as a repository for collaborative information, which may include a variety of information. The nature and sources of the information gathered depend upon the business needs of individual Department organizations and initiatives as well as the laws and policies governing PII.

1.3. Is this a new system or one that is currently in operation?

This is in operation.

1.4. Is this PIA new, or is it updating a previous version? If this is an update, please include the publication date of the original.

New PIA.

1.5. Is the system operated by the agency, by a contractor, or both?

Both authorized CSOSA contractors have access to information in O365, when necessary. Some authorized CSOSA contractors have access to O365 simply as users, and one or more authorized CSOSA contractors has access to certain administrative functions.

2. Legal Authorities and Other Requirements[1]

2.1. What specific legal authorities and/or agreements permit and regulate the collection, and use of the data by the system?[2]

5 U.S.C. § 301; 44 U.S.C. § 3101; 28 CFR Part 800

2.2. System of Records Notice (SORN) Requirement: Is the information in this system retrieved by a name or a personal identifier? If so, this system will need to be covered by a Privacy Act SORN.[3]

O365 is a platform on which Agency employees operated. The purpose of O365 is not to retrieve PII. Information covered by the Privacy Act may be hosted on individual site collections. The covering SORN for each application varies by the mission of the office. It is not possible to anticipate all uses of O365; SORNS will be published for applicable records systems.

2.3. Records Management Requirement: Does a records retention schedule, approved by National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

There is not currently an approved NARA records retention schedule for the system. A records inventory questionnaire has been submitted to the program

[1] If you are unsure of your legal authority, please contact CSOSA's Senior Agency Official for Privacy.
[2] Legal authorities are statutes, executive orders, federal regulations, and/or Memorandum of Understandings. Include the citation/reference of the legal authority.
[3] System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by CSOSA. Verify if there is an existing SORN for the system.

office for submission to the agency's Records Officer. Until a NARA records schedule has been approved, the records will be permanently maintained.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timeliness in the records disposition schedule?

Yes.

2.5. Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed of appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.).

PII could be mishandled due to improper user input, sending/receiving, or non-encryption. To mitigate the risk the component offers training and has implemented the necessary safeguards to protect PII. Email is automatically purged from the system when the email retention policy expires.

3. Characterization and Use of Information

Collection

3.1. Select the specific personal information data elements (e.g. name, email, address, phone number, date of birth, social security number, etc.) that the system collects, uses, disseminates, or maintains.

Identifying Numbers					
Social Security		File/Case ID		Financial Account	
Taxpayer ID		Driver's License		Financial Transaction	
Employee ID		Credit Card			
Other identifying numbers (please specify): -					

General Personal Data					
Name	**X**	Date of Birth	**X**	Religion	
Maiden Name		Place of Birth		Financial Information	
Alias		Home Address	**X**	Medical Information	**X**
Gender		Telephone Number	**X**	Military Service	
Age		Email address	**X**	Physical Characteristics	
Race/Ethnicity		Education			
-					

Work-related Data					
Occupation	**X**	Telephone number	**X**	Salary	
Job title	**X**	Email address	**X**	Work history	
Work address	**X**	Business associates	**X**		
Other work-related data (please specify): -					

Distinguishing Features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Video recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (please specify): -					

System admin/audit data					
User ID	**X**	Date/time of access	**X**	ID files accessed	**X**
IP address	**X**	Queries run	**X**	Contents of files	**X**
Other system admin/audit data (please specify): .					

3.2. Indicate the sources of the information in the system (e.g., individual, another agency, commercial sources, etc.) and how the information collected from stated sources (paper form, webpage, database, etc.).[4]

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	X
Telephone		Email	X		
Other (please specify):					

Government Sources					
Within the Component	**X**	Other CSOSA components	**X**	Other federal entities	**X**
State, local, tribal	**X**	Foreign	X		
Other (please specify):					

Non-government Sources					
Members of the public	X	Public media, internet	X	Private sector	X

[4] Examples include form filling, account verification, etc.

Commercial data brokers					
Other (please specify):					

3.3. Where will the PII be stored in the system?

PII is stored within various components of O365 and primarily on the secure SharePoint and in the cloud.

3.4. Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.).

A potential threat to privacy in light of the information collected is that the system will collect and/or maintain more information than is relevant and necessary to accomplish the Department's official duties. O365 is simply a portal and repository of official communications that does not exercise control over the content of information; however, there are existing technical, administrative, and physical limits on the type of information that may be collected, including but not limited to, the statutory protections afforded certain information under the Privacy Act of 1974, as amended ("Privacy Act"), and CSOSA policy, which limits the type and quantity of information collected to only information that is relevant to accomplish a purpose of the Department.

Purpose and Use of the System

3.5. Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

The information collected, maintained, or disseminated while using O365 is accomplished by the end-user to satisfy their mission requirements and is dependent on what information end-users choose to mail, collaborate with, and instant message. O365 provides end-users with the following primary capabilities:

- Email: The combination of Microsoft Outlook and Exchange provides the ability to manage and exchange electronic messages from one end-user to any other end-user internal or external to the organization or any end-user that has a valid email address outside the organization.
- Calendar: Microsoft Outlook Calendar provides calendar and scheduling for end-users that is fully integrated with email, contacts, and other features. It helps keep

track of appointments, events, and meetings, and can provide end-user schedules for availability.

- Directory: The Active Directory provides a directory that lists entries for every end-user, group, and contact associated with O365. The Active Directory may list first name, middle name, last name, address, city, state, zip code, country/region, title, Component, department, office, assistant, phone numbers (i.e., mobile, pager, home, fax, assistant), organization, employee type, manager, group memberships, and email addresses (i.e., Simple Mail Transfer Protocol, Session Initiation Protocol).
- Instant messaging: Microsoft TEAMS provides the ability to communicate with other CSOSA O365 end-users or a group of CSOSA O365 end-users by utilizing Outlook contacts, which are stored on the Exchange Server. TEAMS provides secure communication for instant messaging, collaboration through desktop sharing, whiteboard documents, PowerPoint documents that participants can share, drawings, graphical annotations, and presentations. TEAMS also offers web conferencing, dial-in conferencing, and Lync meeting scheduling.
- Microsoft Forms: Microsoft Forms provides the ability to create a form, such as a survey or quiz, invite others to respond to it using almost any web browser or mobile device, see real-time results as they're submitted, use built-in analytics to evaluate responses, and export results to Excel for additional analysis or grading.

These capabilities facilitate official communications by allowing CSOSA end-users to share information electronically in real time on the CSOSA network and between authorized devices.

3.6. Select why the information in the system is being collected, maintained, or disseminated.

Purpose			
For criminal law enforcement activities	**X**	For civil enforcement activities	**X**
For Intelligence activities	**X**	For administrative matters	**X**
To conduct analysis concerning subjects of investigative or other interest	**X**	To promote information sharing initiatives	**X**
To conduct analysis to identify previously unknown areas of note, concern, or pattern	**X**	For administering human resources programs	**X**
For litigation	**X**		**X**
Other purpose (please specify):			

Social Security Numbers[5]

3.7. Does they system collect Social Security Numbers? If so, explain the purpose of its

[5] In order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by the law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

collection, type of use, and any disclosures.[6]

No.

3.8. Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

N/A

4. Notice

4.1. How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

Due to the nature of system, the opportunity or right depends on how the information is collected. CSOSA generally does not use O365 to collect information, including PII, directly from the public. However, CSOSA staff and contractors use O365 for business operations in furtherance of CSOSA enforcement or policy mission. To the extent information maintained in O365

CSOSA houses a variety of non-PII information in O365 depending on the needs and purposes of the offices that use this software. Documents that could be created or housed in O365 applications may include a variety of files required in the operation of the agency's mission. The owning office/component is responsible for notifying the individual prior to collecting their information.

Information in O365 pertaining to CSOSA employees and contractors is collected to authenticate end-users and manage administrative business functions including personnel security, human resources, emergency notifications, etc.

4.2. Provide the text of the notice, including where it can be found, or the link to the webpage where notice is posted.

The owning office/component is responsible for notifying the individual prior to collecting their information.

4.3. What opportunities are available for individuals to consent to uses, decline to provide information, or opt-out of this system/project?

Wherever possible, the CSOSA provides timely and effective notice to the public and/or to individuals about activities that impact privacy. For information that is collected pursuant to a request from the CSOSA, notice is provided as part of that

[6] In accordance with OMB Regulations, please note if the system collects SSN, the PIA will require a signature by the Assistant Secretary or equivalent.

request. For those occasions where the CSOSA cannot provide notice at the time the information is collected (e.g., when the information is collected by another law enforcement agency or another organization), the CSOSA provides notice via its Privacy Policy, its Privacy Act system of records notices (SORNs), and its PIAs, including this one.

5. Information Sharing

Internal

5.1. How do agency personnel gain access to the system and the PII (e.g., users, managers, system administrators, developers, contractors, etc.)?

In general, access to data in general is controlled via the built-in access control list (ACL) on a need to access basis. This rule extends to system administrators, developers, contractors as well.

5.2. Will information be shared internally with other CSOSA program offices and/or components, if so, which ones?

Access to O365 is restricted to authorized CSOSA end users. All end users must adhere to the CSOSA Rules of Behavior and take steps to ensure that access to any PII stored in O365 is appropriately limited. Access to the information stored within O365 is dependent on the particular business purpose and the access permissions granted to a specific user.

5.3. What information will be shared and with whom?

Any internal sharing of information varies by the mission of the office or component and is within the scope of the CSOSA's governing regulations.
Recipients of the e-mailed information include approved CSOSA government and contracting personnel.

5.4. How will the information be shared?[7]

Electronically via encrypted email.

5.5. What is the purpose of sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

The purpose of information sharing to the internal offices to support CSOSAs mission and to support the users' daily operations.

5.6. Describe controls that the program offices and/or components have put into place in

[7] Examples, include but is not limited to, case-by-case, direct access, e-mail, etc.

order to prevent or mitigate threats to privacy in connection with the disclosure of information.

The controls and safeguards put into place to prevent and mitigate threat include access control and technical controls. Training is also mandated to ensure proper email and privacy precautions are taken to prevent threats.

All potential CSOSA staff and contractors are subject to background investigation before access is granted. All staff must annually attend privacy and security training. The principle of least privilege is used to grant access to CSOSA staff and contractors, and user actions are tracked in the O365 audit logs.

5.7. Is the access to the PII being monitored, tracked or recorded?

The Office 365 Security & Compliance Center can be used to search the unified audit log to view user and administrator activity in Office 365. The unified audit log allows ISSOs to search for the following types of user and admin activity in Office 365:

- User activity in SharePoint Online and OneDrive for Business
- User activity in Exchange Online (Exchange mailbox audit logging)
- Admin activity in SharePoint Online
- Admin activity in Azure Active Directory (the directory service for Office 365)
- Admin activity in Exchange Online (Exchange admin audit logging)

External

5.8. Will the information contained in the system be shared with external entities (e.g. another federal agency, District of Columbia agency, etc.)?

Any internal and/or external sharing of information varies by the mission of the office or component and is within the scope of the CSOSA's governing regulations. Recipients of the e-mailed information include approved CSOSA government and contracting personnel, various federal agencies, and members of the public.

5.9. What information will be shared and with whom?

Any sharing of information varies by the mission of the office and is within the scope of the Agency's regulations.

5.10. What is the purpose of sharing the specified information with the specified external entity? Does this purpose align with the stated purpose in Question 1.2 above?

If there is any external sharing, the purpose varies by the mission of the office and is within the scope of the Agency's regulations.

5.11. How is the information accessed and used by the external entity?

The way information is shared varies by bureau/office. The email aspects of O365 information to be shared are transmitted via a secure email gateway.

5.12. What controls are in place to minimize risk and protect the data?

CSOSA protects its information resources with a dynamic set of security measures. Some of these measures (e.g., network firewalls, physical security) protect the entire CSOSA enterprise, while other measures (e.g., user access restrictions, encryption) are applied to specific information systems.

5.13. Is the external information sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

Not at this time.

6. Consent and Redress

6.1. How will individuals be notified if there are any changes regarding how their information is being collected, maintained, or disseminated by the system?

The owning office/component is responsible for notifying the individual regarding any changes to their information. The uses of information in O365 are communications to support the various missions of CSOSA.

It would be impracticable to determine in advance every particular communication in which an individual's information will be transmitted as well as to obtain consent for each such communication. The Agency does have notifications in place to inform individuals of potential uses of information, including, but not limited to in its published privacy policy.

6.2. What are the procedures that will allow individuals to access their own information?

Individuals wishing to access and amend Privacy Act covered information maintained by aspects of O365 may contact the office/component that originally collected it. In addition, full instructions for accessing and amending PII held by CSOSA are available at CSOSA's Freedom of Information Act (FOIA) website at https://www.csosa.gov/foia/ . The site also provides complete information on FOIA, the Privacy Act, and related statutes and policies.

6.3. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Procedures vary by the mission of the office or bureau. Individuals should contact the

office or bureau responsible for the initial collection of their information for redress purposes.
.

6.4. How does the project notify individuals about the procedures for correcting their information?

As stated above, In addition, full instructions for accessing and amending PII held by CSOSA are available at CSOSA's Freedom of Information Act (FOIA) website at https://www.csosa.gov/foia/

6.5. How will individuals have the opportunity to consent or dissent to particular uses of the information?

The users' consent to use their PII is the responsibility of the owning office/component.

6.6. How will the agency provide notice to individuals that their PII information may be shared with other agencies or entities (both internal and external)?

Notification is provides through public publication of this PIA. The owning office/component is responsible for notifying the individual prior to collecting their information.

7. Information Security and Safeguards[8]

7.1. Does the component office work with their Chief Information Officer (CIO) to build privacy and security into the system and build privacy extension to the extent feasible?

Yes.

7.2. Do contractors have access to the system?

Yes.

7.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to system data is determined by security and support requirements. Access to collected data is role-based (2 types of user roles – Administration and End-User) on a need-to-know basis. The End-User only has access to content that they created or content that was shared with them. The Administrator has access to all administrative features of O365 depending on the scope of their administration (example, there is an Exchange Administrator, Billing Administrator, SharePoint Administrator, User

[8] If you are unsure which safeguards will apply, please consult with CSOSA's Information Security Officer.

Management Administrator, Security Compliance Administrator, etc). Permissions for Administrator roles adhere to the principle of least privilege and separation of duties so that within O365 admins only have access to the data they require to do their job.

Any network access is granted upon completion of a background security clearance. Users of the system are required to complete mandatory Security, Privacy training; guidance is provided via policy, operation instruction and banners. Least privilege access is provided to align data with work function requirements.

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

Access control is implemented via the secure network; authentication to the system is granted via Active Directory individual and group role membership. In addition, security tools are in place to proactively monitor subject system(s). Controls to prevent the misuse of data include mandatory IT security and privacy training for all Department employees and contractors, privacy training, and the Department's Rules of Behavior for Protecting Personally Identifiable Information (PII).

7.5. Is an Authority to Operate (ATO) required? Has one been granted?

Yes and ATO has been granted, June 9, 2020.

7.6. Is the system able to provide an accounting of disclosures?

Yes.

7.7. What controls are in place to prevent the misuse (e.g., browsing) of data by authorized users who have access to the data?

Technical auditing, monitoring and logging are is in place which enables the prevention and ability to discover unauthorized access or misuse.

7.8. Is there way to identify unauthorized users? If so, what controls are in place to prevent a data breach?

Yes, by the use of technical controls such as audit logs, technical alerts and monitoring.

7.9. Does the agency provide annual security and privacy training for agency employees and contractors?

Yes.

7.10. Who is responsible for assuring safeguards for PII in the system?

All parties are responsible for safeguarding data. The Office of Information

Technology and each user is responsible for the protection, monitoring and handling of the data.

7.11. How will owners of the PII be harmed if privacy data is unlawfully disclosed?

The owners of the information can be subjected to professional or personal harm or embarrassment if data is disclosed.

7.12. If contractors have access to the system, has the agency provided the contractor, who works on the system, a confidentiality agreement or a Non-Disclosure Agreement (NDA)?

Yes.

7.13. What other IT security measures has the agency implemented to protect PII in the system?

Standard security practices are in place which complies with government security requirements and industry best practices. These measures include physical, technical and procedural, to include mandates and guidance from NIST, CISA etc.

8. Auditing and Accountability

8.1. How does the system owner ensure that the information is used in accordance with the stated practices in this PIA?

System owner and the agency ensure that employees and contractor are aware of the agency's privacy policy and risks by ensuring annual security and privacy awareness training. Role based training is required of everyone who has elevated privileges.

8.2. What are the privacy risks associated with this system and how are those risks mitigated?

Risks can vary depending the nature of the threat; however, CSOSA mitigates all Privacy risks by conducting annual risk assessments and full implementation of NIST security and privacy controls.

9. Data Quality and Integrity

9.1. How will the information that the agency collects be verified for accuracy and completeness when it is entered into the system?

Information entered, sent or received in O365 is entered and reviewed at by the user/end-user. The accuracy and completeness is the responsibility of the user/end-user.

9.2. Are there any privacy risks for individuals whose information is collected or used by

the project that relate to data quality and integrity? If so, how will CSOSA mitigate these risks?

Privacy risks are mitigated by annual risk assessments and full implementation of NIST security and privacy controls.

10. Privacy Policy and Statement

10.1. Has the agency provided a privacy statement or policy for this system and is it provided to all individuals whose PII is collected, maintained or stored?

Yes.

10.2. Is the privacy policy publicly viewable? If so where?

The CSOSA privacy policy can be viewed at https://www.csosa.gov/privacy-policy/.

Authorizing Signatures

This Privacy Impact Assessment has been conducted by CSOSA's Office of Information Technology (OIT) and has been reviewed by Sheila Stokes, the Senior Agency Privacy Official, for accuracy.

_____
System Owner Name (Please Print)

JENNIFER EPPS Digitally signed by JENNIFER EPPS Date: 2021.10.19 17:00:47 -04'00'
System Owner Signature Date

Sheila Stokes
Senior Agency Official for Privacy (Print)

SHEILA STOKES Digitally signed by SHEILA STOKES Date: 2021.10.19 17:23:48 -04'00'
Senior Agency Official for Privacy Signature Date

SHEILA STOKES Digitally signed by SHEILA STOKES Date: 2021.10.19 17:24:24 -04'00'
General Counsel (Print)