US Department of Justice

Privacy Impact Assessment
for the

Email and Collaboration Services (ECS)

Issued by:
Morton Posner
JMD Senior Component Official for Privacy

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: October 17, 2024

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 Department of Justice (DOJ) Enterprise Email and Collaborations Services (ECS) provides email, message, and collaboration services. ECS is comprised of the Microsoft 365 (M365) product suite. M365 is a cloud computer-based subscription service offering from Microsoft that provides dedicated enterprise e-mail and collaboration software. M365 provides customers with cloud versions of Exchange Online (EXO), OneDrive (ODB), SharePoint Online (SPO), Teams, Planner, Power Platform, and Exchange Online Protection (EOP).

A Privacy Impact Assessment (PIA) has been conducted because the personally identifiable information (PII) collected, maintained, used, or disseminated by the system includes DOJ user contact information, email messages (including any attachments), instant messages, and audit log information. Even though DOJ users of the system are limited to DOJ employees and contractors, the system captures information about non-DOJ users when non-DOJ users communicate or collaborate with a DOJ user. For example, if a non-DOJ user communicates with a DOJ user via email, the email address of the non-DOJ user, as well as any information transmitted through the email message, will be captured. In addition, in the performance of their duties, DOJ users may transmit information about non-DOJ users via this system, such as during civil or criminal litigation.

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.

The DOJ was one of the first large, federated agencies to transition from multiple disparate email systems to a single, shared, cloud-based infrastructure. In addition to reducing enterprise costs and increasing security, the transition improves user experiences across DOJ offices, regardless of location or device. ECS provides its customers real-time data sharing capabilities and enhanced collaboration, including the following:

(a) Fully auditable and secured cross-Department file collaboration.
(b) Standardized unified communications technology to facilitate mobile communication capabilities.
(c) Critical mission asset protection by improving the security posture throughout the enterprise.
(d) Innovative capabilities to enhance collaboration across the nationwide law enforcement community—between investigative agencies within the Department; state, local, and tribal

law enforcement partners; and external litigators to achieve the Department's mission.

M365 provides customers with cloud versions of Exchange Online (EXO), OneDrive (ODB), SharePoint Online (SPO), Teams, Planner, Power Platform, and Exchange Online Protection (EOP). EXO is a remotely hosted enterprise messaging solution providing email, calendar, and contacts. ODB and SPO store files secured by user-based permissions in the same way they are protected on premises. Teams is a collaboration service that offers chat, audio and video calling and recording, telephone system, on-line meetings, and web conferencing capabilities. Planner provides a permission-based project management tool. Power Platform is a suite of software services, apps, and connectors that work together to turn unrelated sources of data into sets of coherent, visually immersive, and interactive insights. EOP provides antivirus, anti-malware, and anti-spam filtering for email to M365 customers.

In addition, ECS uses security measures such as user-based permissions, passwords, multifactor authentication (MFA), and certificates (e.g., personal identity verification (PIV) cards) to secure electronic data containing PII. Information collected, maintained, used, or disseminated by the system includes user contact information, email messages and attachments, chat, audio and video recording, and audit log information. The underlying information in M365 is dependent on what information DOJ users choose to mail, collaborate with, and chat. All ECS DOJ users must adhere to the DOJ Rules of Behavior.

Access to M365 is restricted to authorized DOJ users (DOJ employees and contractors). M365 leverages Component customers' Active Directory Federation Services (ADFS)[1], which validates DOJ user credentials before authorizing use. ADFS provides single sign-on capabilities for customer identity and authentication.

Information is retrieved by the customer via Outlook, Outlook Web Access, and mobile devices (primarily through a third-party mobile device manager). ECS administrators can retrieve DOJ user account information and audit log information by DOJ username or another DOJ user identifier. DOJ users can retrieve directory information by DOJ user username. Depending on the ECS application used, DOJ users can retrieve information (e.g., information contained in email messages) by name or other identifiers using a full-text search capability. Information is transmitted to and from the system through ZScaler[2] (Cloud Trusted Internet Connection (TIC)[3] and Microsoft Azure ExpressRoute[4]. DOJ data traverses a secure and redundant private virtual network connection using Federal Information Processing Standard (FIPS) 140-2[5] encryption from the DOJ network (JUTNet).

ECS is a DOJ High Value Asset (HVA) with the following interconnections that have

---

[1] Active Directory is a Microsoft directory service for the management of identities in Windows domain networks. *See* https://csrc.nist.gov/glossary/term/active_directory.
[2] ZScaler is covered under separate privacy documentation.
[3] Trusted Internet Connections is a federal cybersecurity initiative intended to enhance network and data security across the Federal Government. See: https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/trusted-internet-connections.
[4] ExpressRoute provides secure connections to Microsoft cloud services. *See* https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction.
[5] NIST FIPS 140-2 can be found at: https://csrc.nist.gov/projects/cryptographic-module-validation-program.

FedRAMP[6] High Authorization to Operate (ATO):

a. Microsoft Cloud Infrastructure Operations (MCIO) provides the physical and logical infrastructure for Microsoft's cloud and hosted applications.
b. Azure Government Services provides the infrastructure, network, storage, data management, and identity management platform on which M365 resides.

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	5 U.S. Code § 301 and 44 U.S. Code § 3101
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

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 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.

[6] The FedRAMP program is a "government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services." More information on the FedRAMP program can be found at: https://www.fedramp.gov.

(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	In most cases, a DOJ user's name is part of creating the DOJ user's Office 365 identity.
Date of birth or age	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Place of birth	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Gender	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Race, ethnicity, or citizenship	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Religion	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Tax Identification Number (TIN)	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2

(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
Driver's license	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Alien registration number	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Passport number	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Mother's maiden name	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Vehicle identifiers	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Personal mailing address	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Personal e-mail address	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Personal phone number	X	A, B, C, and D	Some DOJ users use alternate phone numbers, some of which might be personal phone numbers.

(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
Medical records number	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Medical notes or other medical or health information	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Financial account information	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Applicant information	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Education records	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Military status or other information	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Employment status, history, or similar information	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2

(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
Certificates	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Legal documents	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Device identifiers, e.g., mobile devices	X	A, B, C, and D	Some DOJ users use alternate phone numbers, some of which might relate to a device identifier.
Web uniform resource locator(s)	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Foreign activities	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Juvenile criminal records information	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2

(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
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Grand jury information	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Procurement/contracting records	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Proprietary or business information	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, and D	E911 stores DOJ user's location in the Teams location information service (LIS) database within Microsoft and is not accessible by DOJ users and DOJ-administrators. DOJ users with GFE mobile devices have their location information stored.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2

(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
- **Video containing biometric data**	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
- **Fingerprints**	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
- **Palm prints**	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
- **Iris image**	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
- **Dental profile**	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
- **Voice recording/signatures**	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
- **Scars, marks, tattoos**	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2

(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
- **DNA profiles**	X	A, B, C, and D	Although the system is not designed for this use case, there is still a possibility of data meeting the criteria in Column 2
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A and B	In most cases, a DOJ user's name is part of creating the DOJ user's Office 365 identity.
- **User passwords/codes**	X	A and B	Sending passwords via encrypted email is permitted at DOJ.
- **IP address**	X	A and B	ECS system logs have IP addresses.
- **Date/time of access**	X	A and B	ECS system logs have date/time of access.
- **Queries run**	X	A and B	ECS receives application notifications.
- **Content of files accessed/reviewed**	X	A and B	ECS collects content within its use scope for purposes such as eDiscovery, purges, or other approved searches.
- **Contents of files**	X	A and B	ECS collects content within its use scope for purposes such as eDiscovery, purges, or other approved searches.

(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
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	Teams Recording records and stores Microsoft Teams meetings within the DOJ M365 Environment. Teams meetings include chat transcripts, sent files, audio, and video. By default, Teams Recording is disabled throughout the entire tenant. Teams Recording is enabled for specific DOJ users only with appropriate management approval. Once recording is started, the Teams client displays a warning banner to all others that the current meeting is being recorded. Moreover, Teams Recording only works when the meeting originator has Teams Recording enabled, as well as the person who initiated the recording session.

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):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X

Government sources:					
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): Foreign entities may send/receive emails with DOJ users.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers					
Other (specify): Interconnection in place for 911 Routing in compliance with Ray Baum's Act (FCC Regulation).					

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	X	M365 Platform, by design, is a cloud-based collaboration service.
DOJ Components	X	X	X	M365 Platform, by design, is a cloud-based collaboration service.
Federal entities	X			M365 Platform, by design, is a cloud-based collaboration service.
State, local, tribal gov't entities	X			DOJ components may correspond with state, local, or tribal entities.
Public	X			DOJ components may correspond with the public.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			DOJ components may correspond with courts, parties, witnesses, etc.
Private sector	X			DOJ components may correspond with the private sector.

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 governments	X			Foreign entities may send/receive emails with DOJ users.
Foreign entities	X			Foreign entities may send/receive emails with DOJ users.
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.

ECS information will not be released to the public for "Open Data" or for research or statistical analysis 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.

Generalized public notice has been provided that the account, audit log, and user records maintained in ECS are covered by JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021).

Generalized public notice has been provided that correspondence originating from, received by, or referred to the system are covered by JUSTICE/DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, last published in full at 66 Fed. Reg. 29992 (Jun. 4, 2001), and modified at 66 Fed. Reg. 34743 (Jun. 29, 2001), 67 Fed. Reg. 65598 (Oct. 25, 2002), and 82 Fed. Reg. 24147 (May 25, 2017).

Generalized public notice has been provided that the DOJ directory system information maintained in this system for the purpose of allowing Department personnel to collaborate within the Department and to facilitate professional contacts in order to perform their duties 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, (May 25, 2017).

Other published DOJ SORNs also provide notice, depending on the nature of information in the communication or collaboration document and how the information is retrieved.

In addition, ECS users are presented with a privacy notice as follows:

> "You are accessing U.S. Government information technology and/or information systems which includes: (1) this information technology, (2) this information system, (3) all information technology devices connected to this network, and (4) all devices and storage media attached to this information system or to information technology on this network. This information technology and information system is provided for U.S. Government authorized use only. You have no reasonable expectation of privacy when using this information technology and/or information system and the government may monitor, intercept, search and/or seize data transiting through or stored within. Unauthorized or improper use may result in disciplinary action as well as civil and/or criminal penalties."

Finally, participants in a Teams meeting will be notified by a warning banner when recording is enabled. External users will be prompted with the DOJ Rules of Behavior warning banner when they sign in with guest access to a Microsoft Team in the DOJ tenant.

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.

In most circumstances, DOJ users do not have the opportunity to decline to provide information. All DOJ personnel are required to maintain an ECS account to facilitate email and other information exchanges. As a result, ECS maintains user account information as well as audit log information on all DOJ personnel. In some instances, DOJ users may voluntarily provide information that is collected, stored, and disseminated within ECS. For example, a user may give his/her mailing address to receive DOJ government furnished equipment.

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.

The account, audit log, and user records maintained in ECS can be accessed or amended, in accordance with DOJ regulations, and 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. 37188 (July 14, 2021).

Correspondence originating from, received by, or referred to the system are covered by JUSTICE/DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, last published in full at 66 Fed. Reg. 29992 (Jun. 4, 2001), and modified at 66 Fed.

Reg. 34743 (Jun. 29, 2001), 67 Fed. Reg. 65598 (Oct. 25, 2002), and 82 Fed. Reg. 24147 (May 25, 2017).

The DOJ directory system information maintained in this system for the purpose of allowing Department personnel to collaborate within the Department and to facilitate professional contacts to perform their duties can also be accessed or amended, in accordance with DOJ regulations, and in accordance with 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, (May 25, 2017).

ECS does not exercise control over the content of the communication of end users. As such, to the extent that such communications are protected by the Privacy Act, generalized public notice that the Department is capturing the information has been provided by the various DOJ Privacy Act SORNs[7] that apply to the information depending on its content and how it is retrieved. These documents provide generalized public notice not only to DOJ end-users but also to non-DOJ individuals whose communications or other information may be captured by ECS. Additionally, as noted in Section 7 below, DOJ end-user account information and system administration/audit information is covered by properly published SORNs.

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).

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):** The last approved ATO is dated 9/9/2024 and expires on 9/9/2027. **If an ATO has not been completed, but is underway, provide status or expected completion date: N/A** **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:** All POAMs are tracked in JCAM.
	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:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** M365 is a SaaS managed by Microsoft. On premises supporting assets, e.g., ADFS and AAD connect service are managed by SDS Infrastructure

[7] See https://www.justice.gov/opcl/doj-systems-records.

	team. Vulnerability and configuration scans completed monthly by the Justice Security Operations Center (JSOC).
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:** ECS relies on Microsoft security tools for monitoring and all ECS audit logs are exported to Splunk[8] for monitoring and JSOC review. JSOC responds to anomalies by contacting the ECS team for initial review, and potential remediation or mitigation procedures. By policy, all DOJ systems are subject to periodic audit, evaluation, and re-authorization for compliance with Federal and DOJ security and privacy standards.
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**.
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:** The DOJ Rules of Behavior are part of the mandatory Cybersecurity Annual Training (CSAT). Additionally, Role Based training for administrators and anyone with elevated permissions is conducted annually. ECS does not provide system-specific privacy training.

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?

A full security control assessment has been completed for ECS, to include physical and logical access, identification and authentication, vulnerability management, auditing, and other assessment actions to ensure that security controls are operating as intended. ECS makes use of separate privileged and non-privileged user accounts and leverages additional role-based access control technologies. All system and application log data are sent to DOJ's centralized audit log management system for triage and JSOC review. Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is Federal Information Processing Standard Publication (FIPS) 140-2[9] compliant. Azure Storage encryption is enabled for all new and existing storage accounts and cannot be disabled. ECS makes use of Transport Layer Security (TLS) 1.2 everywhere for data in transit, compliant with FIPS 140-2, to protect data in transit between the browser and the user's workstation and makes use of a redundant private virtual network connection. Emails sent outside of DOJ control can also be encrypted.

The ECS Information Security System Officers (ISSOs) are charged with reviewing logins and

[8] DOJ uses Splunk to collect, store, query, and correlate machine logs. DOJ can use this data to detect and remediate security threats. *See* https://www.justice.gov/d9/2023-01/doj_laas_pia_final_for_publication_1.pdf.
[9] *See* https://csrc.nist.gov/publications/detail/fips/140/2/final.

performing auditing functions to ensure role-based access controls satisfy the above measures. ISSOs re-assess security controls in response to cybersecurity incidents such as breaches, as well as in response to Binding Operational Directives (BODs) issued by the Department of Homeland Security.[10]

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.)

Records in this system are retained and disposed of in accordance with the DOJ Order 0801 Records and Information Management for records created and maintained by Federal agencies related to protecting the security of information technology systems and data and responding to computer security incidents. Log data is maintained in Splunk for 365 days.

In accordance with DOJ Policy Statement 0801.04 Electronic Mail and Electronic Messaging Records Retention, ECS retains data for Capstone users 25 years, and for non-Capstone users 3-7 years, based on Component retention schedules.

In accordance with DOJ Policy Statement 0801.05 Tracking, Storage, and Disposition of Records, the service automatically purges, i.e., permanently deletes, the retained data based on retention schedule.

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. Note: while information pertaining to United States persons is retrievable using this system, whether a component routinely uses the system to do so is a matter that must be determined on a case-by-case basis. Retrievability alone does not make an information system a "system of records" as that term is defined by the Privacy Act of 1974.

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 at 86 Fed. Reg. 37188 (July 14, 2021);

JUSTICE/DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, last published in full at 66 Fed. Reg. 29992 (Jun. 4, 2001), and modified at 66 Fed.

[10] For more information on BODs, *see* https://www.cisa.gov/news-events/directives.

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).

Other published DOJ SORNs depending on the nature of information in the communication or collaboration document and how the information is retrieved.

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 considering, 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 ECS hosts tools, services, and applications that collect PII, and those systems collect other sensitive systems operation information to include names, personal e-mail addresses, personal phone numbers, device identifiers, and system admin/audit data (e.g., user IDs, user passwords, internet protocol (IP) addresses, date/time of actions, queries run, contents of files). JMD's collection and use of PII, as described here and throughout this PIA, poses certain privacy risks. The following steps have been taken to mitigate these risks.

All data retention is managed according to National Archives and Records Administration Federal Records Management, ORMP (Office Records Management Policy) DOJ Order 0801, RIM Directives and associated policies. In accordance with DOJ Policy Statement 0801.04, Electronic Mail and Electronic Messaging Records Retention, ECS retains data for Capstone users 25 years, and for non-Capstone users 3-7 years, based on Component retention schedules. In accordance with DOJ Policy Statement 0801.05 Tracking, Storage, and Disposition of Records, the service automatically purges, i.e., permanently deletes, the retained data based on retention schedule.

Additionally, sources of information come directly from the DOJ user's (government and contractors), systems automatically collecting information, and from external government sources such as other Federal Government agencies where applications hosted on ECS are offered as a

service. To further mitigate risks associated with these activities, ECS implements encryption, account management and access controls, auditing, and system monitoring tools to protect information. For administrators, ECS makes use of separate privileged and non-privileged user accounts and access is granted based on least privilege and need-to-know requirements. DOJ users (government and contractors) will not be provided an opportunity to voluntarily participate in the collection, use, or dissemination of information accessible to ECS Administrators. DOJ users are presented with a warning banner prior to accessing ECS, as well as Privacy Act outlined in Section 5.2. General notice to the public is given through JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021), JUSTICE/DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, last published in full at 66 Fed. Reg. 29992 (Jun. 4, 2001), and modified at 66 Fed. Reg. 34743 (Jun. 29, 2001), 67 Fed. Reg. 65598 (Oct. 25, 2002), and 82 Fed. Reg. 24147 (May 25, 2017) and 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).

To further mitigate privacy risks associated with data sharing activities, ECS uses encryption and logging controls. ECS uses Transport Layer Security (TLS) 1.2 encryption, compliant with FIPS 140-2, to protect data in transit between any M365 DOJ-owned device and ECS and makes use of redundant private virtual network connections. The ECS ISSO performs continuous monitoring of the security controls within the system to ensure security protections are operating as intended. ECS relies on Microsoft security tools for monitoring and all ECS audit logs are exported to Splunk for monitoring and JSOC review. JSOC responds to anomalies by contacting the ECS team for initial review, and potential remediation or mitigation procedures. By policy, all DOJ systems are subject to periodic audit, evaluation, and re-authorization for compliance with Federal and DOJ security and privacy standards.

By Department Order, all DOJ users with access to Department networks, including ECS, must complete DOJ's annual Cyber Security Awareness Training (CSAT). The CSAT course includes information on certain requirements for proper handling of PII. The course identifies potential risks and vulnerabilities associated with using DOJ-owned IT systems, provides a review of the user's role in protecting these systems, and establishes guidelines to follow at work and in remote settings to protect against attacks on IT systems. Additionally, specialized security and privacy awareness training is required annually for privileged users and for managers.

All employees and contractors must also annually sign a DOJ Rules of Behavior agreement confirming that they have completed this course and that they agree to abide by such requirements reviewed in the course. Failure to successfully complete this training can result in termination of the employee or contractor's access to DOJ computers. Participation in the training course is tracked to ensure that DOJ employees and contractors comply with this training.

Records management training is offered to all employees through annual LearnDOJ training. This would include any administrators of the system. Specific records management training for records managers is separate from system personnel.

Finally, to ensure the continued relevance and effectiveness of security controls, the ECS ISSO is responsible for the risk assessments, including privacy and security control assessments annually.

In accordance with the NIST Special Publication 800-53 (Rev.5), these assessments include the management, operational, and technical controls to ensure minimization of privacy risk.