Justice Management Division

Privacy Impact Assessment
for the
DOJ Email and Collaboration Services

Issued by:
[Arthur E. Gary, Senior Component Official for Privacy]

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [July 25, 2017]

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

The United States Department of Justice (DOJ or "Department") Email and Collaboration Services (ECS) is a cloud based Software-as-a-Service (SaaS) model built on the Microsoft Office 365 (O365) Federal Risk and Authorization Management Program (FedRAMP)[1] approved platform. It is an enterprise-class messaging and collaboration solution that allows DOJ to consolidate the email system requirements as well as the collaboration capabilities in a more standardized architecture from a solution, security, and support perspective. ECS provides DOJ Components with cloud versions of Exchange Online (EXO) and Skype for Business (SfB). EXO is a remotely hosted enterprise messaging solution providing email, calendar, and contacts. SfB is a communication service that offers instant messaging, audio and video calling, online meetings, and web conferencing capabilities. ECS will replace the Department's Justice Communication System (JCS).

A Privacy Impact Assessment (PIA) has been conducted because the identifiable information collected, maintained, used, or disseminated by the system includes end-user contact information, email messages (including any attachments), instant messages, and audit log information. Even though end-users of the system are limited to DOJ employees and contractors, the system may capture information about non-DOJ individuals if non-DOJ individuals communicate or collaborate with a DOJ user. For example, if a non-DOJ individual communicates with a DOJ user via email, the email address of the non-DOJ individual, 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 individuals via this system, such as in the course of civil or criminal litigation.

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) The purpose that the records and/or system are designed to serve:

ECS will provide a new email, messaging, and collaboration solution to replace the existing DOJ messaging and collaboration system, JCS. ECS 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 EXO and SfB.

(b) The way the system operates to achieve the purpose(s):

ECS operates to achieve its purposes by providing three main services to DOJ users: email, messaging, and collaboration portals/repositories. EXO is a remotely hosted

[1] 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." FedRAMP, *Program Overview*, https://www.fedramp.gov/about-us/about/ (last visited July 20, 2017). More information on the FedRAMP program can be found at: https://www.fedramp.gov.

enterprise messaging solution providing email, calendar, and contacts. SfB is a communication service that offers instant messaging, audio and video calling, online meetings, and web conferencing capabilities.

(c) The type of information collected, maintained, used, or disseminated by the system:

The type of information collected, maintained, used, or disseminated by ECS includes: user contact information of DOJ end-users and non-DOJ individuals who communicate with DOJ end-users via ECS, email messages (including any attachments), instant messages, audit log information, and information stored in collaboration portals/repositories (such as spreadsheets, word processing documents, and Portable Document Format (PDF) documents). The underlying information in O365 is dependent on what information end-users choose to mail, collaborate with, and instant message, and may include virtually any type of unclassified personally identifiable information (PII), only dependent upon what end-users choose to enter into the system.

(d) Who has access to information in the system:

Access to O365 is restricted to authorized DOJ end-users (DOJ employees and contractors). All end-users who access ECS must adhere to the DOJ Rules of Behavior. Non-DOJ individuals may have access to information in the system only in the sense that they may receive messages from DOJ users containing information (email messages) maintained in ECS.

(e) How information in the system is retrieved by the end-user:

The DOJ end-user uses Outlook, Outlook Web Access and mobile devices (primarily through VMware Airwatch Mobile Device Manager) to retrieve information. ECS administrators can retrieve DOJ end-user account information and audit log information by end-user name or other end-user identifier. DOJ end-users can retrieve directory information by DOJ user name. Depending on the ECS application used, DOJ end-users can retrieve information (e.g., information contained in email messages in the user's inbox or archive) by name or other identifiers using a full-text search capability.

(f) How information is transmitted to and from the system:

ECS transmits information to and from O365 through Microsoft Azure ExpressRoute, a private connection between the DOJ network (JUTNet) and Microsoft Azure data centers (Microsoft Cloud). Traffic traverses JUTNet through Verizon's Secure Cloud Interconnection (SCI) to ExpressRoute using a Transport Security Layer (TLS)

protocol[2] compliant with the Federal Information Processing Standards (FIPS) Publication 140-2.[3] Internal DOJ O365 traffic will traverse ExpressRoute, while Non-DOJ O365 traffic depending upon the service will route through the DOJ Trusted Internet Connection (TIC), which is monitored by the Justice Security Operations Center, or directly by the O365. These interconnections all utilize firewalls, security filtering, and other applicable security measures, as detailed in Section 6, below. Service Delivery Staff (SDS) JUTNet, SDS Network Operations (NetOps) and the FBI Criminal Justice Information Services (CJIS) network teams will manage enterprise wide area and external network connectivity to the DOJ O365 cloud environment

(g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):

The system is an enterprise service and a major system that has interconnections with Component information systems. O365 has the following interconnections that have FedRAMP Provisional Authorization (P-ATO):[4]

- Microsoft Cloud Infrastructure Operations (MCIO)- provides the physical and logical infrastructure for Microsoft's cloud and hosted applications.
- Azure Government Services- provides the infrastructure, network, storage, and data.

(h) Whether it is a general support system, major application, or other type of system:

ECS is a major application capable of offering authorized O365 services.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated.

ECS collects, maintains, or disseminates the following types of information:

- DOJ end-user information: This information includes names and work contact information of DOJ end-users. ECS also maintains logs of end-user activity.

---

[2] The "Transport Layer Security" protocol is used "to secure communications in a wide variety of online transactions" by providing "a protected channel for sending data between the server." National Institute for Standards and Technology (NIST), Special Publication 800-52, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (April 2014), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf.

[3] NIST FIPS 140-2 can be found at: http://csrc.nist.gov/groups/STM/cmvp/standards.html.

[4] A FedRAMP P-ATO is an "initial approval of the [Cloud Service Providers] authorization package by the [Joint Authorization Board] that an executive department or agency can leverage to grant a security authorization and an accompanying [Authorization to Operate] for the acquisition and use of the cloud service within their agency." FedRAMP, *What is a FedRAMP provisional authorization?*, https://www.fedramp.gov/resources/faqs/what-is-a-fedramp-provisional-authorization/ (last visited July 20, 2017).

- Email messages and related information: ECS maintains all email messages sent to or from DOJ end-users, including any attachments. ECS also collects the following items of information regarding non-DOJ individuals who send messages to or receive messages from DOJ end-users via email: name, email address, and message log information (such as internet protocol (IP) address, date of message, and time of message).

- Instant messages: ECS maintains instant messages sent between DOJ end-users.

- Documents uploaded to collaboration portals/repositories: Examples include word processing documents, spreadsheets, and PDF documents.

Email messages, including any attachments, and documents uploaded to collaboration portals/repositories may include significant quantities of personal information relating to substantive work of the Department. Because of the varied nature of the Department's work and because email messages and documents maintained in ECS could conceivably include almost any type of unclassified PII, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated by the system. Therefore, the items of information checked below are limited to end-user information and log information maintained by ECS.

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify):					

General personal data					
Name	**X**	Date of birth		Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address		Medical information	
Gender		Telephone number	**X**	Military service	
Age		Email address	**X**	Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify):					

Work-related data					
Occupation	**X**	Telephone number	**X**	Salary	

Work-related data					
Job title	**X**	Email address	**X**	Work history	
Work address	**X**	Business associates	**X**		
Other work-related data (specify):					

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

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

2.2 Indicate sources of the information in the system. (Check all that apply.)

The sources of the information in the system are as follows:

- DOJ end-user information: The source of DOJ end-user information is existing on-premises identity systems (i.e., Windows Server Active Directory) maintained by the Components. The information is obtained from individuals themselves during the DOJ onboarding process and through the proper authorization forms.

- Email messages and related information: The source of an email message is the sender of the message, who could be a DOJ end-user, an employee of another federal agency, an employee of a state or local government agency, an employee of a private company or law firm, a member of the public, or some other category of individual. Message log information is automatically generated by the system based on the date and time of the message and the IP address from which the message was sent.

- Instant messages: The source of an instant message is the sender of the message, who could be a DOJ end-user, an employee of another federal agency, an employee of a state or local government agency, an employee of a private company or law firm, a member of the public, or some other category of individual.

- Documents uploaded to collaboration portals/repositories: DOJ end-users upload documents to collaboration portals/repositories. Information contained in such

documents may come from any source or sources.

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

Government sources					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign	X		
Other (specify):					

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	X
Commercial data brokers					
Other (specify): The sources of email messages and related information could include any source with email access and knowledge of a DOJ user's email address. While the most likely non-government sources include members of the public, the public media, and the private sector, information collected, maintained, used, or disseminated by ECS could come from virtually any non-government source.					

2.3 Analysis: 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. ECS 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 DOJ policy, which limits the type and quantity of information collected to only information that is relevant to accomplish a purpose of the Department.

Another potential threat to privacy in light of the sources of the information is that there is an increased risk that the collected information is inaccurate because much of the information

maintained by ECS is not collected directly from the subject. As a portal and repository of communications, ECS itself is not the original collection platform for much of the information that it maintains about individuals. For example, many of the documents attached to emails or stored in collaboration repositories for official business purposes—including documents containing information about individuals—were created before they were entered into ECS. While the document creation process may have involved collecting information directly from the subjects of the information, such collection took place outside of ECS. By contrast, DOJ end-user account information (e.g., name, user ID, work contact information) is obtained from existing directories within the Components (which have already been verified for accuracy) or is assigned to the end-user by ECS. In order to mitigate such risks, Department policies require that Components, to the greatest extent practicable upon collection or creation of PII, ensure the accuracy, relevance, timeliness, and completeness of information within the system.

Additionally, because DOJ personnel use ECS to help carry out the Department's various missions, the type of information sent through or stored in the system is not controlled by ECS, but rather is governed by the various authorities delineating Component missions and authorizing the collection and maintenance of information to carry out such missions. These authorities are listed in the various Privacy Act system of records notices (SORNs) that apply to the information in ECS depending on the nature of such information and how it is retrieved. In the SORNs, the agency describes the scope of the categories of records that may be collected as well as the categories of individuals about whom information may be collected. For information about security controls that have been applied to ECS, please see the responses to questions 6.1 and 6.2.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	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		
	Other (specify):		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The information collected, maintained, or disseminated while using ECS is done so 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. ECS 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 global address list (GAL) provides a directory that lists entries for every end-user, group, and contact associated with ECS. The GAL 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 SfB provides the ability to communicate with other DOJ ECS end-users or a group of DOJ ECS end-users by utilizing Outlook contacts, which are stored on the Exchange Server. SfB provides secure communication for instant messaging, collaboration through desktop sharing, whiteboard documents, PowerPoint documents that participants can share, drawings, graphical annotations, and presentations. SfB also offers web conferencing, dial-in conferencing, and Lync meeting scheduling.

These capabilities facilitate official communications by allowing DOJ end-users to share information electronically in real time on the DOJ network and between authorized devices. Because effective communication is essential in accomplishing any objective, the uses described above support the Department's efforts in each of the areas checked in question 3.1.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	5 U.S.C. § 301; 44 U.S.C. § 3101
	Executive Order	
	Federal Regulation	
	Memorandum of Understanding/agreement	

X	Other (summarize and provide copy of relevant portion)	Various DOJ Component mission authorities (including statutes, Executive Orders, and regulations). DOJ Order 0904 – Cybersecurity Program; DOJ Order 2740.1A – Use and Monitoring of DOJ Computers and Computer Systems; DOJ Order 0903 – Information Technology Management; DOJ Order 2880.1C – Information Resources Management Program 1C Chapter 2, section 16. Internet and Intranet Services Management; Service Level Agreements (SLAs)—service agreements between the DOJ, OCIO and its customers that describe service standards, metrics, and reporting (i.e., agreed service terms, targets, and responsibilities).

3.4 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.)

With regard to the substantive information in the system (e.g., email messages, documents uploaded to collaboration portals/repositories, instant messages), ECS is not designated as an official record-keeping system; rather, substantive information in the system is retained and disposed of by the Component in accordance with the retention schedule applicable to such information.

Per the DOJ Cybersecurity Standard, all system administration/audit information is retained for a minimum of 30 days online (in the system itself) and 1 year offline (in backup storage) to support after-the-fact investigations of security incidents. Audit logs may be stored longer upon request if needed for an ongoing matter. This is consistent with General Records Schedule (GRS) 3.2-030, which permits agencies to delete or destroy system files such as "log-in files, password files, audit trail files and extracts, [and] system usage files" when the business use ceases. In general, information is over-written as the storage space is needed. System administration/audit information may include username, computer name, IP address, and type of event. It is treated the same as any other system administration/audit data the system may produce.

O365 is a SaaS cloud platform and does not retain audit records long-term. Microsoft guarantees retention of substantive Department data for 30 days after termination of the cloud platform service agreement and all information is permanently deleted 90 days after termination of service. Audit logs collected by Microsoft are retained in Cosmos, Microsoft's authoritative storage location for ECS audit information, for at least a year to support investigations of security incidents and to meet regulatory retention requirements. O365 scrubs logs of customer

information and hashes it before sending to Cosmos. It can then be imported back into O365 and repopulated back to their original state using a hash to key mapping if an alert or report requires investigation.

ECS retains audit logs online for at least 90 days and, once stored offline by Microsoft in Cosomos, are later accessible for up to a year. Microsoft enables the Department to retain audit logs and records that require longer retention for business use to be pulled by the Department from O365 so that they can be retained in accordance to Department and Component retention policies and procedures. The Department would ingest logs into the Cybersecurity Services Staff (CSS) Splunk[5] instance.

3.5 Analysis: 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 appropriately. (For example: mandatory training for system end-users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats to privacy as a result of the Department's use of the information in ECS include the risks of unauthorized access to the information, threats to the integrity of the information resulting from unauthorized access, and unauthorized disclosure of the information. For a list and description of the security controls that have been put in place to safeguard against these and other risks (including mandatory training for system users regarding appropriate handling of information and automatic purging of information), please see the responses to questions 6.1 and 6.2. Additionally, all end-users are required to sign the DOJ IT Security Rules of Behavior for General and Privileged End-users and to take an annual Cybersecurity Awareness Training (CSAT), which speaks to the disclosure of PII.

Additionally, because of the varied nature of the Department's work and because email messages and documents maintained in ECS could conceivably include almost any type of information, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated by the system. This creates potential risks to the integrity of the information, and potential risks for the unauthorized disclosure of the information. To mitigate these risks, the data is encrypted at rest and in transit and security policies are in place to prevent information that is higher than the categorization watermark from being stored, processed, and transmitted by the system. This is described in the response to question 6.2.

As a result, the Department has put in place certain administrative and technical measures to mitigate these privacy risks. For instance, the Department's data loss prevention

[5] The Department's Splunk Instance captures, indexes, and correlates "real-time" event data in a searchable repository from which IT and information security staff can generate graphs, reports, alerts, dashboards, and visualizations of various events. The Splunk solution provides insight into operational, security, and functional aspects of the environment. More information on Splunk can be found at https://www.splunk.com/.

capabilities block email traffic to external, nongovernment users (i.e., other than .gov or .mil) when a well-formed unencrypted SSN is detected in the body of an email or in an email attachment. The data loss prevention capability also provides notification to the end user that an email was blocked, followed by instructions on how to properly encrypt the email. Alternatively, the data loss prevention capability provides Components with the option to automatically encrypt outbound email traffic when well-formed unencrypted SSNs are detected, rather than automatically blocking the email. Components also have the option to receive periodic event reports when the data loss prevention capability either blocks or automatically encrypts an email. Finally, all DOJ users are required to participate in an annual CSAT course, as well as review and sign DOJ Rules of Behavior, described above. These administrative safeguards provide awareness to ECS users of specific DOJ policies and procedures, which in turn, help mitigate privacy risks.

For a list and description of the security controls that have been put in place in order to prevent and mitigate threats to privacy in connection with the use of information, as well as to safeguard against other threats to privacy, please see the responses to questions 6.1 and 6.2.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	**X**			
DOJ Components	**X**			
Federal entities	**X**	**X (NARA)**		Records are transferred in bulk to NARA when required for record-keeping purposes.
State, local, tribal gov't entities	**X**			
Public	**X**			
Private sector	**X**			
Foreign governments	**X**			
Foreign entities	**X**			
Other (specify):	**X**			Any individual who communications with a DOJ end-user via ECS.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Components utilizing ECS will sign a Risk Acceptance Memo, and must adhere to the ECS SLA, ECS Operations Guide, ECS Design Documentation, and the ECS Security Management Plan while using and implementing O365.

By Department Order, all DOJ users with access to Department networks, including ECS, all individuals at contractor facilities working on Department systems or with DOJ information, and all individuals providing services to the Department, must receive an annual CSAT course. The CSAT course includes information on certain federal information privacy laws, such as the Privacy Act, and 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 mobile settings to protect against attacks on IT systems. 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.

For a list and description of security controls that have been put in place in order to prevent and mitigate threats to privacy in connection with the disclosure of information, as well as to safeguard against other threats to privacy, please see the responses to questions 6.1 and 6.2.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
X	Yes, notice is provided by other means.	Specify how: A warning banner notifies DOJ end-users at login that any information transmitted through the system may be monitored, intercepted, searched, and/or seized by the Department and that users therefore have no reasonable expectation of privacy in

		such information. The Department also has notifications in place to inform individuals of potential collections and uses of information, including, but not limited to, the DOJ website privacy policy, which specifies the collection and use of personal information users voluntarily provide to the Department.[6]
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: 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.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: The vast majority of uses of information in ECS are communications to support the various missions of DOJ Components. 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 Department, however, has notifications in place to inform individuals of potential uses of information, including, but not limited to, the SORNs applicable to the

[6] The DOJ website privacy policy can be found here: https://www.justice.gov/doj/privacy-policy.

		information within ECS, as detailed in Section 7, and the DOJ website privacy policy. Specifically, the website privacy policy paragraphs concerning personal information users voluntarily provide to the Department.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

To provide transparency and allow DOJ end-users to understand how their communications and other information will be handled, a warning banner is displayed on the login screen that DOJ end-users see when they log in to their workstations and mobile devices. ECS utilizes the Component Active Directory implementation of the DOJ-approved standard warning banner. This banner informs users that any information that they transmit through the computer or mobile device, including information transmitted through ECS, may be monitored, intercepted, searched, and/or seized by the Department, and that users therefore have no reasonable expectation of privacy in such communications or other information.

Moreover, 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, notice that the Department is capturing the information is provided by the various DOJ Privacy Act SORNs that apply to the information depending on its content and how it is retrieved. These public documents provide 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: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: October 13, 2016 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:
X	A security risk assessment has been conducted.

X	**Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify:** Microsoft has utilized a FedRAMP Third-Party Assessment Organization (3PAO) to perform an independent security assessment of O365 against a FISMA moderate security baseline. Microsoft provided the DOJ with a Control Implementation Statement Summary Workbook that delineates the security controls that are the customer's (i.e., DOJ's) responsibility. ECS has a security categorization of Moderate. ECS, with guidance from CSS, identified enterprise-level security controls to be implemented and tested by ECS. Security controls identified as the Service Delivery Provider responsibility and are externally inherited at the Department level have established agreements in place (i.e., SLA). To the extent possible, DOJ Common Controls and hybrid security controls have been inherited from existing systems and programs to reduce the assessment effort and streamline the Security Assessment and Authorization process. The security controls that have been identified, tested, and implemented to protect against risks identified in the security risk assessment include those listed in DOJ Security Assessment and Authorization Handbook v. 8.4, which provides the framework and direction for performing security assessments and authorizations of all DOJ IT systems, as well as those listed in response to question 6.2. ECS is responsible for maintaining the enterprise security Authorization to Operate (ATO) of O365, but the Component must accept the risk associated with allowing O365 to, in any way, utilize Component data. Additionally, Components have some implementation and testing responsibility when leveraging the enterprise ATO.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The ECS Team, in coordination with Microsoft, has been consistently monitoring, testing, and evaluating the system and controls that have been applied to the system throughout the system's deployment and migration of services. DOJ IT security standards, which include monitoring, testing, and evaluation requirements, as well as Microsoft best practices, have been applied to the system. See the response to question 6.2 for additional information on monitoring, testing, and evaluation.
X	**Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information**: Audit logs are maintained to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. Audit logs can only be accessed by authorized staff as required to ensure compliance with security requirements. Microsoft retains audit records in Cosmos for 1 year to support investigations of security incidents and to meet regulatory retention requirements. Additional information on Microsoft auditing procedures is detailed in their system security plan and can be found in the O365 with International Traffic in Arms Regulation (ITAR) Support (F1402113099). ECS is currently implementing Splunk, which will function as the audit log retention and generation tool.
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.

	The following training is required for authorized end-users to access or receive information in the system:	
	X	General information security training
	X	Training specific to the system for authorized end-users within the Department.
		Training specific to the system for authorized end-users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

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

- ECS has a security categorization of FISMA Moderate. Microsoft has given O365 a security categorization of FedRAMP Moderate. Microsoft has assessed and implemented all applicable security controls for a FedRAMP Moderate baseline. ECS has assessed and implemented all applicable security controls deemed the customer's (i.e., DOJ's) responsibility for a FISMA Moderate baseline.
- The system is accessible by DOJ employees and contractors only and utilizes tiered/role based access commensurate with the end-user's official need to access information. Physical access to system servers is controlled through site-specific controls and agreements. Microsoft manages all software and hardware for O365 as a SaaS system.
- The system 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 (including DOJ Order 0904 and FIPS 140-2).
- All email communication will use TLS that is FIPS 140-2 compliant and validated cryptomodule for confidentiality and integrity.[7] ECS will use Microsoft Azure ExpressRoute,[8] which allows DOJ to extend the JUTNet network into O365 over a dedicated, private connection facilitated by Verizon's SCI private IP Multiprotocol Label Switching network. The existing Verizon SCI connection provides a dedicated connection to O365. DOJ firewalls have access control lists that are source/destination and port and protocol specific. JUTNet enforces route filtering to ensure only traffic destined for Microsoft networks can be routed through this connection.
- All users must complete computer security awareness training annually, as well as read and agree to comply with DOJ information technology Rules of Behavior both prior to accessing the DOJ network and annually thereafter. System administrators must complete additional professional training, which includes security training.
- Audit logging is configured and logs are maintained separate from other system data to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. Audit logs can only be accessed by authorized users with privileged access. System administration/audit data is

[7] *See supra* notes 2–3.
[8] *See supra* Section 1(f).

automatically purged at defined intervals and in accordance with applicable retention periods.

Potential unauthorized disclosures or data breaches are covered in vendor contracts and the DOJ Rules of Behavior in order to ensure appropriate procedures and reporting.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created, or has been created, in accordance with the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: • 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); • JUSTICE/DOJ-002, Department of Justice Computer Systems Activity and Access Records, last published in full at 64 Fed. Reg. 73585 (Dec. 30, 1999), and modified at 66 Fed. Reg. 8425 (Jan. 31, 2001), and 82 Fed. Reg. 24151, 153 (May 25, 2017); and • Other published DOJ SORNs depending on the nature of information in the communication or collaboration document and how the information is retrieved.
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

System administrators can retrieve DOJ end-user account information and audit log information by end-user name or other end-user identifiers. DOJ end-users can retrieve directory information by DOJ end-user name. Depending on the ECS application used, DOJ end-users can retrieve information (such as information contained in email messages) by name or other identifiers using a full-text search capability.