Drug Enforcement Administration

Privacy Impact Assessment
for the
SharePoint

Issued by:
James Robert Bryden
DEA Senior Component Official for Privacy

Approved by: Kameron Cox
Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: September 3, 2026

(May 2022 DOJ PIA Template)

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.)

SharePoint is a browser-based collaboration system allowing DEA employees to work and communicate within an access-controlled environment. The system provides workspaces for employees to share content (documents, data, surveys, etc.) and collaborate based on job related requirements.

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.

SharePoint is an online collaboration system allowing DEA employees to communicate and work together more effectively and automate business processes which can aid in boosting productivity. SharePoint also allows for the development of automation through online forms, workflow documentation, and the approval/denial of multiple types of requests, in accordance with the team collecting those approvals. DEA's goal in deploying SharePoint is to foster information sharing, collaboration, and resource sharing; to improve standards and governance throughout DEA; and to incorporate enterprise portal solutions on a single, centralized platform.

SharePoint is part of the Email and Collaboration infrastructure built into DEA main Information Technology (IT) infrastructure, called Firebird. Firebird is an on-premise/cloud hybrid, General Support System (GSS) environment with strictly limited interfaces/connections to non-Department of Justice (DOJ)/Drug Enforcement Administration (DEA) resources or external networks. Firebird utilizes the DOJ Justice Unified Telecommunications Network (JUTNet) for Wide Area Network (WAN) connectivity. (See Firebird PIA for additional information). Firebird also hosts DEA's Enterprise-wide operating system, MS Office 365, its included applications (e.g., MS Word, Excel, etc.) and several Email and Collaboration Services (ECS) programs common to all users, of which SharePoint is one.

The following list outlines the many different types of sites offered to DEA individuals, teams and business units:

- Intranet Sites: Content that is accessible by anyone in DEA. Modification of content is limited to designated users and administrators. Intranet webpages generally contain little to no sensitive information such as third-party names, physical and personal email addresses,

or personal phone numbers. However, some intranet sites may contain organizational chart and duty station information of DEA employees.

- Team Sites: Permission-based sites exclusive to teams, divisions, or sections; ensure end-users with access have a need-to-know clearance with ascending levels of permission to view or edit the content within the site
- Project Sites: A time or event limited collaboration site used to track and manage projects from inception to production. Access is granted by designated individuals in the project to those with a need-to-know to create, view, and modify content.[1]
- OneDrive - A personal site for individual users to store documents and other work products. Documents and folders can be shared with users and user groups on a need-to-know basis for those files. Individuals sharing files are not sharing the entire OneDrive environment, only the files as indicated.

SharePoint is not intended to be a repository for original or official records and generally serves as a platform for employees to share working copy versions of records and drafts of records with one another.

SharePoint sites are created and controlled by the DEA Enterprise SharePoint Development and Operations team and tracked through either the Firebird on-premises server farm at the system administration level, or, within the DOJ 365 Azure tenant. DEA employees do not have the capability to create their own sites.

See Appendix A for a listing of the largest and most used SharePoint sites at DEA.

Additionally, data collection in SharePoint is carried out in a variety of ways; lists, online forms, surveys, documentation management and wikis. All collections are stored in designated SharePoint sites. All data deemed as "sensitive" are housed in team sites, project sites, and OneDrive here access is only granted to those who have a need-to-know basis. "Sensitive data" can include, but not limited to, HR-related information such as the employees' names, titles, years of service, phone numbers, and tactical gear and firearm serial numbers. OneDrives may contain virtually any preliminary drafts of documentation created by or filled out by an individual DEA staff member. With respect to SharePoint sites established by teams, units or sections, the webpage may contain working drafts of important case-related or subject matter documentation and drafts of work product for which multiple authors may need to provide input. In the case of law enforcement related SharePoint sites, DEA investigatory documentation, such as drafts of Reports of Investigation, intelligence reports, may be present as well as working copies of relevant records of arrest, operation plans, or associated administrative form required to be filed for investigations, among others.

Access to information in a team site is granted to DEA employees through a request process – SharePoint provides a request link allowing requestors to fill in a justification for gaining access. Those requests are forwarded to either the Site Collection Administrator (SCA) or the Enterprise SharePoint Administration team in order to review and approve that the employee

[1] For purposes of this PIA, project sites and Teams sites will be collectively referred to as "Teams sites"

has the proper credentials to review/modify information and approved. There are multiple SCAs and Site Points of Contacts throughout the agency who have the ability to grant access to team or division members requesting access to a team site.

SharePoint is both an on-prem housed platform as well as a cloud-based platform program. On-prem housed systems are running within the Firebird network; SharePoint Online sites are maintained within the Department of Justice's Azure tenant. All Firebird users are required to read and sign the DOJ Rule of Behavior (ROBs) prior to getting access to the network. SharePoint sites on DEA Networks are searchable but the content of the site is only visible to users having pre-determined access to that site. Depending on circumstances team sites may be deemed undiscoverable via internal agency searching due to farm[2] level administration applied restrictions. This action is taken by request of the Site Owner if the site houses sensitive information and therefore should not be discoverable.

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	• The Comprehensive Drug Abuse Prevention and Control Act of 1970 (Controlled Substances Act), 21 U.S.C. § 801 et. seq., • 28 U.S.C. § 534 • 40 U.S.C. § 11101 • 44 U.S.C. § 3101
	Executive Order	
	Federal Regulation	Attendant regulations of the Controlled Substance Act: 21 C.F.R. § 1300, et seq.
	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 particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

[2] A collection of one or more servers that work together to run the **SharePoint** platform

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C and D	Names of employees, contractors, detailees, other federal government personnel and/or members of the public (US and non-USPERs) likely to be collected and stored.
Date of birth or age	X	A, B, C and D	Date of birth or age information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs) likely to be collected and stored.
Place of birth	X	A, B, C and D	Place of birth information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs) may be collected and stored.
Sex	X	A, B, C and D	Sex information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs) likely to be collected and stored.
Race, ethnicity or citizenship	X	A, B, C and D	* See note at end
Religion	X	A, B, C and D	* See note at end
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C and D	Truncated SSNs or Full SSNs of employees, contractors, detailees, and/or other federal government. Any SSN of member of the public, (US or non-USPERs) may be collected and stored.
Tax Identification Number (TIN)	X	A, B, C and D	* See note at end
Driver's license	X	A, B, C and D	* See note at end
Alien registration number	X	A, B, C and D	* See note at end
Passport number	X	A, B, C *and* D	* See note at end
Mother's maiden name	X	A, B, C and D	* See note at end
Vehicle identifiers	X	A, B, C and D	* See note at end

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Personal mailing address	X	A, B, C and D	Personal contact information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs) likely to be collected and stored.
Personal e-mail address	X	A, B, C and D	Personal contact information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs) likely to be collected and stored.
Personal phone number	X	A, B, C and D	* See note at end
Medical records number	X	A, B, C and D	* See note at end
Medical notes or other medical or health information	X	A, B, C and D	* See note at end
Financial account information	X	A, B, C and D	Financial data of employees, contractors, detailees, other federal government and/or personnel members of the public (US or non-USPERs) may be collected and stored.
Applicant information	X	A, B and C	*See note at end
Education records	X	A, B, C and D	* See note at end
Military status or other information	X	A, B, C and D	* See note at end
Employment status, history, or similar information	X	A, B, C and D	* See note at end
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C and D	* See note at end
Certificates	X	A, B, C and D	* See note at end
Legal documents	X	A, B, C and D	* See note at end
Device identifiers, e.g., mobile devices	X	A, B, C and D	* See note at end
Web uniform resource locator(s)	X	A, B, C and D	*See note at end
Foreign activities	X	A, B, C and D	*See note at end
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C and D	Criminal records information of employees, contractors, detailees, and/or other federal government. Any SSN of member of the public, (US or non-USPERs) likely to be collected and stored
Juvenile criminal records information			

(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
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C and D	* See note at end
Whistleblower, e.g., tip, complaint or referral			
Grand jury information	X	A, B, C and D	* See note at end
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C and D	* See note at end
Procurement/contracting records	X	A, B, C and D	* See note at end
Proprietary or business information	X	A, B, C and D	Business contact information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs) likely to be collected and stored.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C and D	*See note at end
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C and D	* See note at end
- **Video containing biometric data**	X	A, B, C and D	* See note at end
- **Fingerprints**	X	A, B, C and D	* See note at end
- **Palm prints**	X	A, B, C and D	* See note at end
- **Iris image**	X	A, B, C and D	* See note at end
- **Dental profile**	X	A, B, C and D	* See note at end
- **Voice recording/signatures**	X	A, B, C and D	* See note at end
- **Scars, marks, tattoos**	X	A, B, C and D	* See note at end
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C and D	* See note at end
- **DNA profiles**	X	A, B, C and D	* See note at end
- **Other (specify)**	X	A, B, C and D	* See note at end
System admin/audit data:			
- **User ID**	X	A and B	User IDs of employees, contractors, detailees and/or other Federal government personnel available in Audit logs.
- **User passwords/codes**	X	A and B	User passwords/codes of employees, contractors, detailees and/or other Federal government personnel available in Audit logs.

(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
- **IP address**	X	A and B	IP addresses of employees, contractors, detailees and/or other Federal government personnel available in Audit logs.
- **Date/time of access**	X	A and B	Dates/time of system access by employees, contractors, detailees and/or other Federal government personnel available in Audit logs.
- **Queries run**	X	A and B	Queries run by employees, contractors, detailees and/or other Federal government personnel available in Audit logs.
- **Content of files accessed/reviewed**	X	A and B	Records accessed by employees, contractors, detailees and/or other Federal government personnel.
- **Contents of files**	X	A and B	Records accessed by employees, contractors, detailees and/or other Federal government personnel available in Audit logs..
Other types (please list all other types of identifying information collected and describe as completely as possible):	X	A, B, C and D	* Because users may store any work product or other information in SharePoint files, it is possible that any personally identifying information of employees, contractors, detailees, other federal government personnel and/or members of the public (US or non-USPERs) could be collected and stored, but collection of such information is not the intended purpose of the system.

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	X	Hard copy: mail/fax	X	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):					

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

Section 4: Information Sharing

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

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	Case-related or sensitive information is shared within team sites and access is granted based on the user status.
DOJ Components	X			Case-related or sensitive information is shared within team sites and access to other DOJ personnel may be granted based on the user status and a need to know.

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.**
Federal entities	X			Other Federal entities do not have direct SharePoint access. However, if SharePoint has information related to an investigation that is relevant to a different investigation by non-DOJ entities, that evidence may be shared with investigators working on the second investigation, consistent with the provisions of SORN Justice/DEA-008, routine use "a" or as allowed in DOJ regulations, the disclosure provision in a relevant Court Order, the agreement or MOU with the party that granted access or provided the information or other applicable information sharing policy.
State, local, tribal gov't entities	X			These entities do not have direct access to the SharePoint. However, if SharePoint has information related to an investigation that is relevant to a different investigation by non-DOJ entities, that evidence may be shared with investigators working on the second investigation, consistent with the provisions of SORN Justice/DEA-008, routine use "a" or as allowed in DOJ regulations, the disclosure provision in a relevant Court Order, the agreement or MOU with the party that granted access or provided the information, or other applicable information sharing policy.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Public	X			The public does not have direct access to the SharePoint. However, if deemed important to share information from SharePoint with the news media or members of the public (e.g., for their protection) some information may be exported and shared on a case-by-case basis. Such information could also be subject to Freedom of Information Act disclosures.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			These entities do not have direct access to the SharePoint. However, any information in SharePoint relevant to litigation is subject to a hold and may be exported and shared as part of the evidentiary discovery process and may be presented in a court of law as evidence.
Private sector				
Foreign governments	X			These entities do not have direct access to the SharePoint. However, any information in SharePoint relevant to foreign partner nations may be shared on a limited basis.
Foreign entities				
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.

Not Applicable.

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.

No notice is provided to users upon entering information into the SharePoint application. Notice has been provided generally through the publication in the Federal Register of Systems of Records Notices. See below:

JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 Fed. Reg. 37188 (July 14, 2021);

JUSTICE/DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (June 4, 2001);

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

Information in SharePoint is taken from other DEA systems that have collected it. Other published OPM, DOJ, and DEA SORNS, depending on the nature and subject matter of each collaboration document within a SharePoint team site, including, but not limited to, Human Resources related documents (e.g., SORNs OPM GOVT-001 to 005, etc.), Civil and Criminal Investigations (e.g., SORNs DEA-008, DEA-010, DEA-012, etc.), and Security and Intelligence matters (SORNs DOJ-006, DEA-013, and DEA-INS-111 etc.). See Section 7.2 for a full listing of SORNs potentially applicable to the system from which the working copies of SharePoint information were taken or into which the finalized documents drafted though SharePoint are uploaded.

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

Information is not directly collected from non-DEA employees by SharePoint. Most information in SharePoint related to investigations was collected by other systems. In most circumstances, those law enforcement information collection systems have no opportunities for individual consent. However, general notice of the existence, contents, and uses the information relating to the public contained SharePoint information taken from other DEA systems will be provided by the publication of the PIAs and the SORNs for the systems of record from which the underlying data was taken.

In addition, when law enforcement agents and officers interact with individuals in connection with an investigation, the subjects are generally aware that their information will be recorded and stored. Furthermore, information is frequently collected through other lawful means, such as by subpoenas and search warrants. If information is obtained from individuals through Federal Government-approved forms or other means, such as information collected pursuant to seizures of property, or notices on forms that state information may be shared with law enforcement entities.

Overall, SharePoint is a web-based document management and storage system that facilitates collaboration and information sharing. Information supplied to SharePoint by users is generally

voluntary. However, in the event a survey or data collection opportunity is required, participation is solicited but not mandated unless DEA administrative or operational management (e.g., Executive Office or Human Resources, etc.) is requesting the information.

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.

Access to information is granted to DEA employees through a request process – there is a request link allowing requestors to fill in a justification for gaining access. Those requests are forwarded to either the Site Collection Administrator (SCA) or the Enterprise SharePoint Administration team in order to review and approve that the employee has the proper credentials to review/modify information and approved.

Members of the public may seek records stored in SharePoint via the Freedom of Information Act (FOIA) or the Privacy Act (PA). Such requests are subject to appropriate FOIA and PA exemptions.

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):** N/A. SharePoint is not a standalone platform. It is integrated into the Firebird network and rests within DEA browsers. Per the Information System Division CISO, SharePoint does not require its own ATO. (See also, JMD Email and Collaboration Systems (ECS) PIA: https://www.justice.gov/d9/pages/attachments/2019/08/20/ecs_pia_final_7-25-2017.pdf) Firebird is under the "Ongoing Authorization" program for its ATO. **If an ATO has not been completed, but is underway, provide status or expected completion date**: N/A
X	**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:** Any risk or POA&Ms related to SharePoint fall within the Firebird ATO boundary.

X	**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:** Any risk or POA&Ms related to SharePoint fall within the Firebird ATO boundary and privacy control implementation are acknowledged through the Firebird ATO.
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** The applicable security impact category for the system is High because it is part of Firebird which was assigned the High category.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** DEA monitors the information system on a continuous basis for changes to the information system or its operational environment, the information system security and privacy plan boundaries, or other conditions. DEA conducts security impact analyses of system associated changes, update of the information system's security plan and other relevant information system documentation, such as the system privacy plan, as appropriate, throughout the information system's lifecycle DEA reports changes in the security or privacy status of the system to appropriate officials on a regular basis. Significant changes to the system require reauthorizations by the DEA Authorizing Official. Significant changes that affect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are reviewed and assessed by the CPCLO, or a duly authorized official, prior to reauthorization by the Authorization Official. DEA ensures that the appropriate officials are made aware, in a timely manner, of information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement.
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:** The application audit logs are reviewed daily as part of the Cybersecurity Operations, Response and Engineering Unit (TCVV) review process. The audit logs are reviewed based off alerts received from Splunk, Crowd strike, and Vectra which occur when an alert is activated. Operations & Response team reviews all logs forwarded from DEA systems for suspicious behavior and notifies the system owner/security points of contact of any alerts. DEACORE reviews alerts received from Vectra and Crowd strike that feeds into the log management tool and contact the system owner. Additionally, the program management office performs periodic reviews to ensure user and system behavior comply with all applicable DOJ, DEA, and federal guidelines, policies, and laws. DEACORE is not responsible for dictating the periodic review. The system owner is

	responsible for complying with all guidelines, policies, and laws; The ISSO for Relativity is responsible for validating that users comply with said governance while TCVV enforces actions based upon an infraction (cybersecurity incidents, policy violations). TCVV performs validation for compliance to governance during risk assessments which are scheduled (ATO renewal or continuous monitoring audit) or remediation efforts against the system during a cybersecurity investigation.
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**. As a standard operating procedure, all contracts have the necessary, proper and accurate Privacy Act clauses and language required listed in each contract awarded within DEA.
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:** Security and Privacy Act training is conducted annually and throughout the year in order to provide an overview of agency employees' obligations to protect PII. The component has a requirement for all employees, including contract employees, to complete the mandated Cyber Security Awareness Training annually.

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. **<u>Administrative Controls</u>:**

There are multiple Site Collection Administrator (SCAs) and Site Points of Contacts (POCs) throughout the agency who have the ability to grant access to team or division members requesting access to a team site. These roles only apply to the site they oversee. They must have the proper permissions to grant the access and vet the request prior to granting access. Per DEA SharePoint Governance policies, each SCA must monitor access and ensure vulnerabilities to data security, if any, are eliminated – i.e., SCAs are responsible for maintaining the integrity of site and site collections. See Appendix A for a listing of the largest and most used SharePoint sites at DEA.

b. **<u>Technical Safeguards</u>:**

The SharePoint application is accessible only through successful login to Firebird, which is managed by Firebird Active Directory and requires a PIV card. Once a successful login is granted, individual SharePoint team sites also require individual permissions based on a need-to-know approval. Access to each individual team site is managed by the respective user with admin privileges. That user is responsible for ensuring that any requester has a need-to-know for the information contained within the Teams site prior to granting access. While access is

granted to Firebird, another level of access control is adhered to through permissions management within every site setting.

All SharePoint data stored, processed or transmitted within the Firebird maintains end-to-end encryption.

c. Physical Protections:

SharePoint access is limited to users authenticated to the Firebird network. Firebird is accessible via wired network connection, Firebird wireless, or remote virtual private network. Physical access to Firebird wired and wireless is managed via perimeter fences, PIV accessible external gates and/or PIV accessible external and internal doors, and guards. All guests of DEA facilities must sign in/out and are subject to escort of guards. Access control to Firebird VPN requires possession of and access to a Firebird laptop, which is useable only with PIV. All Firebird laptops are encrypted with FIPS 140-2 compliant encryption.

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.)

SharePoint is not a repository for original or official records and serves as a platform for employees to share working copy versions of records and drafts of records with one another. While there is no specific retention schedule for SharePoint, individual sites have the ability to implement retention policies that are specific for the content of the site.

As such, deletion of SharePoint sites falls in line with the records lifecycle – sites are reviewed annually and based on extended periods of no utilization or no up-to-date content, are deleted and no longer accessible so that unused content is not sitting dormant on DEA servers or in the cloud tenant. In rare instances that SharePoint stores original versions of official records, those records will be governed by the appropriate records retention schedule as applicable.

Per DEA SharePoint Governance policy, it is the responsibility of individual Site Administrators and Points of Contacts to review the sites they own to ensure their sites are up to date and remove unused/obsolete pages or sites and remove from the inventory/servers. In addition, SharePoint farm administrators run reports on sites that have been unused or dormant and the SharePoint team works with the administrators to either update or remove such sites.

Section 7: Privacy Act

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

_____ No. __X___ Yes.

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

JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 Fed. Reg. 37188 (July 14, 2021);

JUSTICE/DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (June 4, 2001);

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

Other published OPM, DOJ, and DEA SORNS may be applicable depending on the nature and subject matter of each collaboration document within a SharePoint team site, including, but not limited to:

Human Resources related documents--

- OPM GOVT-001,General Personnel Records, 77 Fed. Reg. 79694 (Jun. 19, 2006)
- OPM GOVT-002 Employee Performance File System Records, 71 Fed. Reg. 35347 (Jun. 19, 2006)
- OPM GOVT-003 Records of Adverse Actions, Performance Based Reductions In Grade and Removal Actions, and Terminations of Probationers, 71 Fed. Reg. 35350 (Jun. 19, 2006)
- OPM GOVT- 005GOVT-5 Recruiting, Examining and Placement Records, 71 Fed. Reg. 35351 (Jun. 19, 2006)
- JUSTICE/DEA-015, Training Files, 52 Fed. Reg. 47182, 217 (Dec. 11, 1987)

Civil and Criminal Investigations, including criminal intelligence activities—

- DOJ-005, Nationwide Joint Automated Booking System (JABS), 71 Fed. Reg. 52821 (9-07-2006)
- JUSTICE/DEA-003, Automated Records and Consolidated Orders System- Diversion Analysis and Detection System (ARCOS-DADS), 69 Fed. Reg. 51104 (Aug. 17, 2004)
- JUSTICE/DEA-005, Controlled Substances Act Registration Records (CSA), 52 Fed. Reg. 47182, 208 (Dec. 11, 1987)
- JUSTICE/DEA-008, Investigative Reporting and Filing System, 77 Fed. Reg. 21808 (Apr. 11, 2012)
- JUSTICE/DEA-011, Operations Files, 52 Fed. Reg. 47182, 214 (Dec. 11, 1987)
- JUSTICE/DEA-012, Registration Status-Investigation Records, 52 Fed. Reg. 47182, 215 (Dec. 11, 1987)
- JUSTICE/DEA-017, Grants of Confidentiality Files (GCF), 52 Fed. Reg. 47182, 218 (Dec. 11, 1987)
- JUSTICE/DEA-020, Essential Chemical Reporting System, 52 Fed. Reg. 47182, 219 (Dec. 11, 1987)

- JUSTICE/DEA-021, DEA Aviation Unit Reporting System, 65 Fed. Reg. 24986, 987 (Apr. 28, 2000)
- JUSTICE/DEA-022, El Paso Intelligence Center (EPIC) Seizure System (ESS), 71 Fed. Reg. 36362 (Jun. 26, 2006)

Security and Inspections files--

- DOJ-006, Personnel Investigation and Security Clearance Records for the Department of Justice, 67 Fed. Reg. 59864 (Sep. 24, 2002)
- JUSTICE/DEA-010, Planning and Inspection Division Records, 52 Fed. Reg. 47182, 213 (Dec. 11, 1987)*;
- JUSTICE/DEA-013, Security Files, 52 Fed. Reg. 47182, 215 (Dec. 11, 1987)

General Administrative matters—

- DOJ-001, Accounting Systems for the Department of Justice, 69 Fed. Reg. 31406 (Jun. 03, 2004)
- DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, 77 Fed. Reg. 26580 (May 4, 2012)
- DOJ-007, Reasonable Accommodations for the Department of Justice, 67 Fed. Reg. 34955 (May 16, 2002)
- DOJ-008, Department of Justice Grievance Records, 68 Fed. Reg. 61696 (Oct. 29, 2003)
- DOJ-009, Emergency Contact Systems for the Department of Justice, 69 Fed. Reg. 1762 (1-12-2004)
- DOJ-015, Department of Justice Employee Assistance Program (EAP) Records, 77 Fed. Reg. 5570 (Feb. 3, 2012)
- DOJ-016, Debt Collection Enforcement System, 77 Fed. Reg. 9965 (Feb. 21, 2012)
- DOJ-017, Department of Justice, Giglio Information Files, 80 Fed. Reg. 16025 (Mar. 26, 2015)
- Justice/JMD-003, Department of Justice Payroll System, 69 Fed. Reg. 107 (Jan. 2, 2004)
- Justice/JMD-017, Department of Justice Employee Transportation Facilitation System, 66 Fed. Reg. 20683 (Apr. 24, 2001)

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?

a. Potential Threats Related to Collection of Information

Privacy Risk: Due to the large number of law enforcement related working copies in SharePoint, individuals whose PII is collected may not receive notice nor participate in collection, use, or dissemination of their PII in this system, in most cases.

Mitigation: This risk cannot be mitigated in most cases. Because working copies and drafts in the system will often be used for law enforcement purposes and contain sensitive information related to criminal and civil investigations, it is not feasible or advisable to permit individuals to access, correct or amend any investigative PII in this system. Such information is either information is consensually obtained via interviews or proper process has been obtained through administrative subpoenas, search warrants, or seizures subsequent arrest or a lawful exception to obtaining process. With respect to employee PII collected for HR or administrative reasons, DEA employees do have a method under the Privacy Act and Freedom of Information Act (FOIA) to access and seek amendment though procedures set forth on DEA FOIA website.

Privacy Risk: Some PII collected and input into SharePoint may not be directly relevant and necessary for DEA to accomplish its purpose or mission, such as belonging to an unrelated individual not under suspicion.

Mitigation: This risk is partially mitigated. SharePoint is only a collaboration space where information downloaded into its files has already been collected by other DEA systems. To the extent that the PII previously collected was not necessary or is irrelevant, the collection determination made was outside the scope of SharePoint's purposes or operations. However, the following measures generally help ensure that evidence collected by DEA and input into any system is both relevant and necessary for the investigation: (1) extensive training on the proper collection of relevant evidence given to criminal investigators; (2) investigative procedures and policies detailing the proper collection of evidence; and (3) supervisory involvement in all aspects of the investigation, including collection of evidence. If evidence collected is found not to be relevant, such evidence will be marked as not relevant and/or segregated from the relevant evidence, likely never to be accessed again.

b. <u>Potential Threats Related to Use and Maintenance of the Information</u>

Privacy Risk: Unauthorized DEA personnel may gain incorrect access control thus allowing them to modify PII being stored within the site.

Mitigation: This risk is mitigated by SCAs limiting "Full" access control to individuals who have completed the proper training and acknowledged the Rules of Behavior guidance prior to gaining that access. Additionally, access to the use of site information is not granted to individuals unless they have been vetted and justified in having access.

Privacy Risk: SharePoint sites storing PII, if no longer utilized, will remain active and accessible thus allowing for information to remain in existence without a set retention purge date.

Mitigation: This risk is partly mitigated, as per SharePoint Governance policy, site owners are notified when they create a site that they must delete individual sites when no longer needed. SharePoint administrators provide additional oversight by conducting periodic manual reviews to identify and purge dormant SharePoint sites.

Privacy Risk: Outsiders may access SharePoint sites due to insufficiently implemented Physical, Technical, and Administrative security and privacy controls.

Mitigation: This risk is mitigated through proper implementation of the security and privacy controls referenced above in Section 6.3. Further, SharePoint is protected from insider threats and malicious, external engineering attacks by DEA's threat monitoring technology. Security measures in place to safeguard sharing of information include: IT monitoring tools; firewalls; intruder detection and data loss prevention mechanisms; and system audit logs. In addition, DEA has established minimum auditable events based on DOJ IT security requirements. Given that SharePoint files do not have direct connections to the Internet and cannot be shared outside of DEA proprietary digital infrastructure (called Firebird)), therefore, the risk of compromise to privacy data within the system by malicious intent or malware is low. Consistent with FISMA and NIST security controls, transmissions of DEA non-public data occur only through secure methods, e.g., Virtual Private Networks (VPN), Transport Layer Security (TLS), or other encryption.

Privacy Risk: DEA may use outdated or incomplete duplicative data on a SharePoint site for operations or decisions that may not align with the final/official records contained in the official systems of records elsewhere.

Mitigation: This risk is mitigated. It is a standard DEA procedure to mark clearly when documents are preliminary drafts. Important documents, such as Reports of Investigation, must be signed, therefore once finalized, it is clear when versions saved in SharePoint would merely be working copies.

c. <u>Potential Threats Related to Dissemination of the Information</u>

Privacy Risk: DEA personnel may share or disclose PII to an inappropriate party or for improper use.

Mitigation: This risk is partly mitigated because SharePoint does not have the technical capacity to transfer data outside of the agency. All external sharing must be manually exported prior to sharing. DEA users may only share within Firebird's SBU and PII data as defined in section 4.1 of the PIA. Externally, PII may only be shared with other federal, state, and local entities when subject to a valid routine use or Privacy Act exception. By DEA policy, Any dissemination to outside agencies would generate a DEA-381 Disclosure Account Record, in which sharing is logged and justified All DEA employees receive annual Privacy Act training which informs them of proper PII handling, including proper disclosures.

Privacy Risk: The system's administrative controls may be insufficient to prevent unauthorized individuals within DEA from accessing the system's PII without a need to know.

Mitigation: Although an insider threat with access to PII in SharePoint files could accidentally or maliciously disclose the information accessed, this risk is mitigated because most SharePoint team sites are constrained to a limited number of team members. Those individuals are approved access by the designated Site Collection Administrators (SCAs), who know the sensitivities of the data and which personnel should be granted access, thereby ensuring an assessment of a requester's need to know. To address inadvertent disclosure, DEA Rules of Behavior make clear that PII may only be shared within DEA when the receiving party has a

valid business “need to know” the information. SharePoint administrators do not only vet the justification for access but also ensure users are adhering to governance policies and are responsible for monitoring and removing access when an employee leaves the team, division, or agency. Further, DEA uses the following governance and audit metrics:

- While SharePoint links can be shared, access cannot. Individuals receiving links will not be able to access the shared content unless initial access has been granted by an SCA.
- SharePoint generates audit reports that can provide details on hits by employees to sites, pages and information. Unique hits can be monitored and addressed if out of the ordinary.
- Governance policies mandate that SharePoint administrators monitor the site collection for unusual activities. SharePoint administrators are trained in monitoring and maintenance.

APPENDIX A: SHAREPOINT TOP UTILIZED AND CONTENT ORIENTED AGENCY SITES

Top Utilized SharePoint Sites:

- DEA Today
  - DEA News and highlights stemming from both the field and Headquarters
- DEA Webster
  - Central point of agency information, HR, policies, procedures and application links
- Counter Threat
  - Site used for the field to centralize threat information and develop operational details
- Policy Portal
  - Central repository for policy and policy directives
- Business Operations
  - Business Operations platform encompassing participating Divisions and placemats

SharePoint Team Sites containing significant amounts of PII/Sensitive Information

- Human Resources Division
  - Site used to house org charts, awards and self-inspection documentation
- Information Systems Division
  - Past performance plans and telework agreement documentation
- Employee Equal Opportunity Office
  - Complaint processing documents, DOJ and EEOC reporting
- Office of the Administrator
  - Media request and location/POC information
- Miami Division
  - Property management, TFO assignment and Inspections
- Office of Inspections
  - Domestic stat reports/bulk waivers and budget reports
- DEA Intelligence Program
  - Events and Intelligence Oversight Board Reporting information

- Diversion Control Division
  - FOIA and Diversion Control correspondence trackers; purchasing, funding, travel and property
- San Diego Division
  - Command and control center, conference room scheduling and investigative resources
- Omaha Division
  - Go-By documentation (e.g., Quick Reference Guides), student volunteer program and Trauma Team Members
- Office of Finance
  - Org chart, staff members, images and logos, FOIA request information
- Office of Public Affairs
  - Hiring actions, performance appraisals, Form SF-52s
- New Jersey Division
  - Employee and position information, emergency contact information and employee phone list
- Washington Division
  - Enforcement, Go-By documentation, asset forfeiture and firearm details
- Counternarcotic Cyber Investigation Task Force
  - Subpoena Tracking, Go-By's and Form DEA-19 documentation