TAX DIVISION

Privacy Impact Assessment
for the
TAX OFFICE AUTOMATION SYSTEM
TAX-OAS

Issued by:
Carmen M. Banerjee and Dara B. Oliphant
TAX Co-Senior Component Officials for Privacy

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

Date approved: December 18, 2020

Section 1: Executive Summary

The Tax Division (TAX) is a litigating component of the United States Department of Justice (DOJ). TAX's mission is to enforce the nation's tax laws fully, fairly, and consistently, through both criminal and civil litigation. The Tax Division Office Automation System (TAX-OAS) is an office automation system that enables TAX managers, attorneys, and non-attorney personnel the ability to collect, organize, analyze, and disseminate information.

TAX maintains several systems and applications within TAX-OAS that permit it to carry out its mission. (Please see Section 2 and the Appendix to this PIA for a listing and brief summaries of the systems and applications) Specifically, TAX-OAS encompasses the computing environment, including almost all computing platforms, applications, and internal data networks under the control of TAX. The TAX-OAS is comprised of the following system components: workstations and peripherals - desktop and laptop computers, certain personal digital assistants, scanners and printers; application software - custom applications such as TaxDoc and HR solutions, off-the-shelf business-specific applications such as Financial Management Information System (FMIS), customized off-the-shelf applications such as Interwoven/iManage document management solutions, standard Microsoft office automation software, and system management utilities; servers and mass storage - file and print servers, directory and authentication servers, messaging platforms, and disk and tape storage solutions; and network connectivity - routers, switches, and a copper and fiber cabling plant to interconnect all TAX office areas via an Internet Protocol (IP) network. The OAS also includes interface equipment to external networks where necessary.

For purposes of this PIA, TAX defines all of the following as employees: Federal staff, detailees, volunteers/interns, and contractors. Employees are the sole users of the TAX-OAS System, and the applications residing on it, except for occasional use by partnering government agency personnel, as limited and described in this PIA. From an infrastructure standpoint, TAX-OAS applications and services are available to TAX personnel in a hybrid cloud environment which uses a mixture of on-premise and Federal Risk and Authorization Management Program (FedRAMP) compliant government cloud hosting options such as Microsoft and Amazon Web Services. Decisions on the selected hosting infrastructure are based on several factors, including cost, resources, security/access, bandwidth/load, web development, testing, backups, Continuity of Operations (COOP), and administrative maintenance. All infrastructure is aligned with National Institute of Standards and Technology (NIST) security standards, IRS Publication 1075, and with the Federal Information Technology Acquisition Reform Act (FITARA).

TAX prepared a Privacy Impact Assessment for the TAX-OAS because TAX-OAS collects and disseminates information in identifiable form about individuals. TAX employees, contractors, and members of the public who are involved in TAX's litigation, administrative, civil and criminal matters, and otherwise transact business with TAX are amongst the individuals whose PII the TAX-OAS collects and/or transmits.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The TAX-OAS network spans seven locations. Three locations are TAX office locations in the Washington, DC metro area; two nearby locations are data centers, which reside outside of Washington, DC. One location is a shared-DOJ space in Landover, MD, and the last location is a TAX office in Dallas, TX. TAX is currently developing a cloud presence in Amazon Web Services as an additional network location. All locations are connected to each other using the JUTNET network which is hosted by JMD to provide secure communications between sites.

TAX OAS consists of a suite of systems and applications and corresponding sub-systems and modules. The systems and applications suite include Microsoft Active Directory, TaxDoc, Human Resources System (HRS), Interwoven (iManage) Document Management System (DMS), TaxNet Intranet, Automated Litigation Management, and Annual Bar Membership Submission (ABMS). For a full description of these systems and applications, please see appendix A.

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
X	Statute	Title 18 of the U.S. Code, certain sections including §§ 1341, 1344; Title 26 of the U.S. Code, certain sections including § 6103(h)(2), (h)(4); 28 U.S.C. § 2410 and §§ 514-19; 31 U.S.C. § 5314; 5 U.S.C. § 552.
	Executive Order	
X	Federal Regulation	28 C.F.R. §§ 0.70, 0.71; 28 C.F.R. § 16.41
X	Agreement, memorandum of understanding, or other documented arrangement	Joint Statement between DOJ and the Swiss FDF executed in 2013, https://www.justice.gov/tax/swiss-bank-program
X	Other (summarize and provide copy of relevant portion)	Justice Manual Title 6: Tax, 6-1.000 through 6-7.000, https://www.justice.gov/jm/title-6-tax

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.

(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); Members of the Public - Non-USPERs*	*(4) Comments*
Name	**X**	**A, B, C, D**	Names of DOJ contractors, employees, and other federal government personnel such as those applying to jobs at TAX. Names of taxpayers, witnesses, and other individuals involved in litigation handled by TAX employees. A small group within TAX collects names from members of the public when they submit requests for records about themselves invoking FOIA and the Privacy Act, because they must submit a certification of identity (DOJ form 361), or a written authorization comporting with DOJ's FOIA/Privacy regulations.
Date of birth or age	**X**	**A, C, D**	Date of birth of DOJ contractors, employees, and other federal government personnel such as those applying to jobs at TAX. Dates of birth and ages of taxpayers, witnesses, and other individuals involved in litigation handled by TAX employees. A small group within TAX collects dates of birth from members of the public when they submit requests for

(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); Members of the Public - Non-USPERs*	*(4) Comments*
			records about themselves invoking FOIA and the Privacy Act, because they must submit a certification of identity (DOJ form 361), or a written authorization comporting with DOJ's FOIA/Privacy regulations.
Place of birth	**X**	**A, C, D**	Place of birth of DOJ contractors, employees, and other federal government personnel such as those applying to jobs at TAX. A small group within TAX collects places of birth from members of the public when they submit requests for records about themselves invoking FOIA and the Privacy Act, because they must submit a certification of identity (DOJ form 361), or a written authorization comporting with DOJ's FOIA/Privacy regulations.
Gender	**X**	**A**	Gender information of DOJ employees.
Race, ethnicity or citizenship	**X**	**A, C, D**	Race, ethnicity, and citizenship of DOJ employees and contractors. Race, ethnicity, and citizenship of taxpayers, witnesses, and other individuals involved in litigation handled by TAX employees. As to citizenship, a small group within TAX collects citizen status from members of the public when they submit requests for records about themselves invoking FOIA and the Privacy Act, because they must submit a certification of identity (DOJ form 361), which asks to citizenship

(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); Members of the Public - Non-USPERs*	*(4) Comments*
			status.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	**X**	**A, B, C, D***	Social Security Numbers of DOJ contractors, employees, and other federal government personnel such as those applying to jobs at TAX. TAX legal staff collects financial information from taxpayers who owe money to the IRS (pre-suit to determine whether a case should be settled or for a post-judgment collection); it collects the information through a form and a notice that requests, but does not require, Social Security Numbers of the taxpayers. The legal staff might also collect social security numbers and taxpayer information numbers as part of materials produced to us in discovery in our legal cases. Those materials might come from the parties to our cases, the Internal Revenue Service, other federal agencies, or third parties. *A small group within TAX collects Social Security Numbers from members of the public when they submit requests for records about themselves invoking FOIA and the Privacy Act, if they choose to include their SSNs within their requests or within a certification of identity (DOJ form 361), or a written authorization comporting with DOJ's FOIA/Privacy regulations.
Tax Identification Number (TIN)	**X**	**A, B, C, D**	As to members of the public (USPERS, and possibly non-USPERS)

(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); Members of the Public - Non-USPERs*	*(4) Comments*
			(a)Tax identification numbers of expert witness contractors and other vendors. (b) Government assigned identifiers of taxpayers who are parties and possibly non-parties relevant to civil and criminal matters TAX handles. It is feasible, however, that a tax identification number may be captured as part of the Automated Litigation Support processes through the electronic discovery application (e.g., automated document review databases). The workspaces in which documents with this information are captured and stored (Document Management System, automated review databases), require assigned restricted access.
Driver's license	**X**	**A, B,C, D**	As to members of the public (USPERS, and possibly non-USPERS), some first-party FOIA requesters, consistent with applicable FOIA regulations, submit a copy of their driver's license to verify their identities. It is feasible, however, that a tax identification number, driver's license, alien registration number, or passport number may be captured as part of the Automated Litigation Support processes through the electronic discovery application (e.g., automated document review databases). The workspaces in which documents with this information are captured and stored (Document Management System,

(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); Members of the Public - Non-USPERs*	*(4) Comments*
			automated review databases), require assigned restricted access.
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers	**X**	A, C, D	Members of the public (USPERS, and possibly non-USPERS) (a) Non-employee visitors, TAX may temporarily capture vehicle information for temporary permit parking purposes. (b) Parties and relevant non-parties to the legal matters TAX handles (see Note). The legal staff may collect vehicle information from or about taxpayers who owe money to the IRS. That information would possibly be included in a listing of assets. TAX employees who have parking permits in the DOJ buildings in which they work.
Personal mailing address	**X**	A, B, C, D	Personal mailing addresses of DOJ employees and other federal government personnel such as those applying to jobs at TAX. Address information of taxpayers, witnesses, and other individuals involved in litigation handled by TAX employees. A small group within TAX collects personal mailing addresses from members of the public when they submit requests for records about themselves invoking FOIA and the Privacy Act, because they must submit a certification of identity (DOJ form 361), or a

(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); Members of the Public - Non-USPERs*	*(4) Comments*
			written authorization comporting DOJ's FOIA/Privacy regulations.
Personal e-mail address	**X**	A, B, C, D	Personal e-mail addresses of DOJ employees, and other federal government personnel. E-mail addresses of taxpayers, witnesses, and other individuals involved in litigation handled by TAX employees. A small group within TAX collects personal e-mail addresses from some members of the public when they submit requests for records invoking FOIA or the Privacy Act about third parties or themselves if and when they submit FOIA requests through TAX's general box for the public to electronically submit these records requests, or possibly otherwise include their personal e-mails in these requests submitted in forms other than through e-mail (e.g., fax or hard copy mail).
Personal phone number	**X**	A, B, C, D	Personal phone numbers of DOJ employees and other federal government personnel. Phone numbers of taxpayers, witnesses, and other individuals involved in litigation handled by TAX employees. A small group within TAX collects personal phone from some members of the public when they submit requests for records invoking FOIA or the Privacy Act about third parties or themselves and they chose to include their personal phone

(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); Members of the Public - Non-USPERs*	*(4) Comments*
			numbers in these requests submitted in through e-mail, or fax or hard copy mail.
Medical records number			
Medical notes or other medical or health information	**X**	A, C, D	Health information or records of TAX employees are not routinely sought after or collected in a data fields housed within the TAX OAS. However, copies of material containing health information may be provided to members of the Human Resources staff or managers, and if so, would be stored in the Document Management System. The Human Resources staff maintains a secure electronic folder in the Document Management System application within TAX OAS, where the following types of files are housed: health care-related documents provided by employees for purposes of satisfying requirements under the ADAA; EEO settlements; FMLA and sick leave administration; and workplace issues arising from the COVID-19 pandemic. It is remotely feasible that information related to medical conditions exists in the Human Resources System also within the TAX-OAS. Access to the health-related information and/or documents is restricted to the appropriate management officials, TAX's employment counsel, the appropriate HR staff, and the Human Resources Director. Health information or records about taxpayers involved in civil or criminal matters TAX handles are not specifically sought after or collected in a

(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); Members of the Public - Non-USPERs*	*(4) Comments*
			data fields housed within the TAX OAS. In isolated incidents, however, it is feasible that some medical/health-related information may be provided by individuals involved in litigation and/or captured as part of the Automated Litigation Support processes through the electronic discovery application. The workspaces in which documents with this information are captured are stored (Document Management System, automated review databases) require assigned restricted access.
Financial account information	**X**	A, C, D	Income information, and monetary reimbursement for work-related matters such as training, is stored in the HRS application. Income of current government employees outside of DOJ from whom TAX has obtained pre-employment information. As to members of the public, (USPERS, and possibly non-USPERS), TAX collects financial information from parties who owe money to the United States (pre-suit to determine whether a case should be settled or for a post-judgment collection). Conversely, when TAX needs to make payments to taxpayers, it often collects bank routing data so that we can pay them. TAX also collects financial information in conjunction with criminal investigations of individuals alleged to be evading taxes. This information may

(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); Members of the Public - Non-USPERs*	*(4) Comments*
			include the identity of accounts, transfers, and various financial services that taxpayers procure from both foreign and domestic financial institutions.
Applicant information	**X**	A, B, C	Applicant information of DOJ employees, other federal government personnel, and potentially members of the public (e.g., information submitted as part of the employment application process).
Education records	**X**	A, B, C	Education records of DOJ employees, contractors, expert witnesses, and potentially members of the public (e.g., information submitted as part of the employment application process). Education records of taxpayers, parties, and possibly non-parties relevant to civil and criminal matters TAX handles.
Military status or other information	**X**	A, C	Military information of DOJ employees, contractors, and potentially members of the public (e.g., information submitted as part of the employment application process). Military records of taxpayers, parties, and possibly non-parties relevant to civil and criminal matters TAX handles.
Employment status, history, or similar information	**X**	A, C	Employment status, history, or similar information of DOJ employees, mostly submitted as part of the employment application process. Education and employment information of contractors and expert witnesses.

(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); Members of the Public - Non-USPERs*	*(4) Comments*
			Employment status or similar information of members of taxpayers and other parties relevant to civil and criminal matters TAX handles.
Employment performance ratings or other performance information, e.g., performance improvement plan	**X**	A, B, C	Supervisory and Human Resources information related to the performance or other performance information of TAX employees is maintained in the Human Resources System and the Document Management System within TAX OAS.
Certificates	**X**	A, B, C	Certificates of DOJ employees and potentially members of the public (e.g., information submitted as part of the employment application process).
Legal documents			
Device identifiers, e.g., mobile devices	**X**	A	TAX tracks information about the work phones, tablets and laptops it issues to employees. Note: Otherwise, electronic device identifiers are not information specifically sought after or collected in a data field housed within the TAX OAS. In isolated incidents, however, it is feasible that some device identifier information may be captured as part of the Automated Litigation Support processes through the electronic discovery application.
Web uniform resource locator(s)	**X**	A	Web uniform resource locators of DOJ employees.
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	**X**	A, B, C, D	Criminal records information pertaining to TAX employees. The records or information collected or maintained as they are provided or identified during the pre-employment or employment security process. Documents involved in the

(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); Members of the Public - Non-USPERs*	*(4) Comments*
			security processes are kept in the DMS in secure folders. Criminal records information is also potentially collected about parties and witnesses involved in the litigation and prosecution TAX handles. As to members of the public, criminal records information or civil law enforcement information, (possibly including non-USPERS) are collected and maintained in the TAX-OAS including the Document Management System related to TAX's Criminal Enforcement and Civil Trial tax matters. Additionally, TAX maintains and uses criminal records information about parties, witnesses, and non-parties, which may be captured as part of the Automated Litigation Support Management processes.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	**X**	A, B, C, D	TAX's Civil Trial, Criminal Enforcement, and Appellate sections collect civil law enforcement information, including allegations of civil law violations. The primary manner in which TAX collects this information is the referrals and accompanying material from several bureaus of the Department of the Treasury (primary bureau is the Internal Revenue Service), and from TAX's own discovery processes.
Whistleblower, e.g., tip, complaint or referral	**X**	A, B, C, D	Because the civil and criminal matters TAX handles are referred from several bureaus of the Department of the

(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); Members of the Public - Non-USPERs*	*(4) Comments*
			Treasury (primary bureau is the Internal Revenue Service), the referring bureau materials TAX receives can include whistleblower information.
Grand jury information	**X**	A, B, C, D	TAX's Criminal Enforcement sections collect grand jury information.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	**X**	A, B, C, D	TAX's Criminal Enforcement sections collect information concerning witnesses to criminal matters
Procurement/contracting records	**X**	A, B, C	Procurement/contracting records of DOJ employees and contractors, other federal government personnel, and business address of members of the public.
Proprietary or business information	**X**	A, B, C, D	Business information of DOJ employees, contractors, other federal government personnel, and business addresses of members of the public (US and non- USPERs).
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
Photographs or photographic identifiers			
Video containing biometric data			
Fingerprints	**X**	A	TAX digitally takes the fingerprints of a small percentage of employees to obtain or renew certain security clearances. It processes and transmits the fingerprints to another component for further processing.
Palm prints			
Iris image			
Dental profile			
Voice recording/signatures			

(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); Members of the Public - Non-USPERs*	*(4) Comments*
Scars, marks, tattoos			
Vascular scan, e.g., palm or finger vein biometric data			
DNA profiles			
Other (specify)			
System admin/audit data:	**X**	A	System admin/audit data of DOJ employees and contractors.
User ID	**X**	A	User ID of DOJ employees and contractors.
User passwords/codes	**X**	A	User passwords/codes of DOJ employees and contractors.
IP address	**X**	A	IP addresses of DOJ employees and contractors.
Date/time of access	**X**	A	Date/time of access of DOJ employees and contractors.
Queries run	**X**	A	Queries run of DOJ employees and contractors.
Content of files accessed/reviewed	**X**	A	Content of files accessed/reviewed of DOJ employees and contractors.
Contents of files	**X**	A	Contents of files of DOJ employees, and contractors.
Other (please list the type of info and describe as completely as possible):			

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	*Online	X

Government sources:					
*Online only Division attorneys-see Appendix					
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					
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	Employees within TAX receive restricted access to information as needed, at a role-based permission level. For example, electronic case files related to civil and criminal cases and matters are accessible to those employees assigned to handle or supervise those cases or matters. DMS and TaxDoc are interconnected and the information or files related to a specific matter or case within these systems is only available to individuals assigned those specific matters or cases. If information is created by an individual and not related to a case, then all files are private by default and

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.**
				only accessible and shared by the owner of the information. Personal information that is not related to a case file is only accessible to those individuals who are responsible for handling that matter, for example, HR matters are restricted to those who are authorized to access the information. Sensitive non- case information more likely to contain PII, such as personnel related records, are only accessible to select personnel within TAX.
DOJ Components	X	X		Exported data is transferred on a case-by-case basis or via a bulk transfer and is used to create a record in DOJ's Consolidated Debt Collection System (CDCS), where the information is stored/maintained. Exported data is transferred on a case-by-case basis or via a bulk transfer and is used to create a record in DOJ's Unified Financial Management System (UFMS), where the information is stored/maintained. Statistical data reports and GPRA data calls, with PII data excluded, are transferred on a case-by-case basis or via a bulk transfer. Compliance Screens from agencies, which contain addresses on a case-by-case basis or via a bulk transfer. TAX shares human resources data with OARM and various offices within JMD on a case-by-case basis or via a bulk transfer in limited circumstances.

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.**
				TAX's Civil Trial, Criminal Enforcement, and Appellate sections need to share information with U.S. Attorney Offices nationwide and other DOJ offices, including INTERPOL, FBI to carry out their duties on a case-by-case basis. TAX's Civil Trial, Criminal Enforcement, and Appellate sections need to share information to carry out their duties as they relate to work with foreign governments or foreign entities through Office of Foreign Litigation at the Civil Division and the Office of International Affairs at the Criminal Division on a case-by-case basis. *See* Foreign Governments and Entities sections below for details.
Federal entities	X			TAX's Civil Trial, Criminal Enforcement, and Appellate sections need to carry out their investigatory, litigation, and prosecutorial duties by sharing PII with partnering agencies including the Internal Revenue Service, the Treasury Inspector General for Tax Administration, the Special Inspector General for Investigation in Afghanistan Reconstruction, and the U.S. Postal Service.
State, local, tribal gov't entities	X			TAX's Civil Trial, Criminal Enforcement, and Appellate sections may share PII with state and local entities to carry out their duties.
Public	X			Logs of FOIA requests submitted to TAX with PII data excluded, and press releases, are posted to public-facing web presence (i.e., Justice.gov). Select information may be disclosed in public litigation filings, in accordance with statutes and Federal Rules of Procedure.

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.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Select information is shared with counsel, parties, witnesses, and courts or other judicial tribunals for litigation purposes on a case-by-case basis.
Private sector				
Foreign governments	X			TAX's Criminal Enforcement sections may need to share PII with a foreign government when for example, it indicts a foreign person, or attempts to reach assets or histories of individuals, or takes discovery. TAX works through the Office of International Affairs at the Criminal Division pursuant to either a Treaty, a Mutual Legal Assistance Treaty or similar official agreements to carry out its duties. Sometimes TAX provides PII of an accountholder to one of the banks participating in the Swiss Bank Program in order to ascertain penalties against a bank. When TAX's Civil Trial sections' need to obtain discovery from foreign governments pursuant to the Hague Convention, TAX shares PII and does so through the Office of Foreign Litigation at the Civil Division.
Foreign entities	X			An example of the type of foreign entity with whom TAX needs to share PII is FINMA, the Swiss Financial Market Supervisory Authority.

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

No.

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.

As set forth below, TAX provides individuals with generalized notice about its needed collection, use, and sharing of PII through a variety of Systems of Records Notices (SORNS), and in other circumstances, individualized notice Privacy Act section 552a(e)(3) notices.

TAX provides individualized notice to individuals completing employment-related forms required for employment (e.g., background investigations) seeking PII by DOJ and TAX by way of the 552a(e)(3) notices attached to government-wide official forms. It also provides notice through SORNS issued by TAX (Justice/TAX 003), and SORNS issued DOJ-wide and government-wide.

TAX provides generalized notice to individuals involved in the civil cases and matters through its SORN Justice/TAX 002. As to the sub-set of individuals who owe money to the IRS (pre-suit to determine whether a case should be settled or for a post-judgment collection), TAX provides a Privacy Act (e)(3) notice with Form 433-A, which it uses to collect financial information from individuals. TAX provides notice to individuals involved in its criminal enforcement cases and matters through its SORN Justice/TAX 001. Moreover, applicable court processes would notify individuals involved in civil or criminal court matters.

If another domestic federal agency is involved in the investigation or litigation of civil or criminal enforcement matters, that agency's SORN would provide generalized, and under some circumstances, individualized, notice that the information may be shared with the DOJ for the purpose of a civil or criminal investigation or litigation.

Finally, individuals who are involved in TAX's administrative and other operational matters, TAX provides generalized notice to individuals through the applicable SORNS listed in Section 7 of this PIA.

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.

Opportunities exist for TAX employees to optionally provide information associated with their profile in the personnel locator application. Additionally, as part of onboarding procedures TAX employees are presented with the opportunity to acknowledge a background investigation, including credit check, as part of the process. TAX employees also provide optional PII via the following forms: SF-181 (Ethnicity and Race Identification); SF-144 (Statement of Prior Federal Service); SF- 1152 (Designation of Beneficiary); SF-256 (Self Identification of Disability); DOJ-543 (Employee Locator

Form); DOJ-555 (Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act); AD-349 (Employee Address); and state-specific tax withholding forms.

For information related to investigations and litigation matters, opportunities for individuals to participate in the collection, use or dissemination of information must be through court order, warrant, subpoena, discovery requests, voluntary submissions (e.g., Freedom of Information Act (FOIA) or Privacy Act requests/correspondence), and other such legal means. An opposing party may challenge the relevance of the information and not produce the information in litigation, but that challenge would be determined before the information is collected and maintained by the TAX-OAS system.

Unless individuals are opposing parties in litigation, or voluntarily submit information (e.g., FOIA or Privacy Act requests/correspondence), individuals do not provide information directly to TAX for use in the TAX-OAS system. Individuals who are opposing parties in litigation can object to TAX obtaining the information through the discovery process. Individuals whose information is collected in the course of litigation involving an additional entity, such as another government agency or business, may have the opportunity to consent at the time of collection from the other entity.

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.

Individuals seeking to gain access to information within an application housed on the TAX-OAS system, request amendment or correction of their respective information, and/or receive notification of the procedures, may do so by making a FOIA and/or Privacy Act request by following the provisions of those statutes and DOJ regulations on those statutes. Further instructions on how to submit a request are provided on TAX's FOIA webpage (https://www.justice.gov/tax/foia).

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):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** *12/22/2020*

	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: *TAX-OAS has completed its annual assessment of security controls in the Cyber Security Assessment and Management (CSAM) application. TAX is currently renewing its three-year ATO that was last issued on 12/22/2017 with an expected completion date by 12/22/2020. This will certify TAX's ability to maintain FIPS (Federal Information Processing Standards) and FISMA compliant IT systems.*
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** *Monitoring functions have been implemented and are conducted on a constant basis at the perimeter of the environment, as well as within the internal network. The system security is tested and evaluated on a bi-annual basis, in support of operational and regulatory requirements.*
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:** *Auditing functions have been implemented at both the network and application levels. All actions within the environment are continuously tracked and reviewed for unusual activities. TAX's Office of Information Technology (OIT) utilizes automated log collection, aggregation, reporting and alerting tools in order to more efficiently review security and audit logs. These tools highlight and alert issues to appropriate TAX OIT personnel in real-time. Additionally, manual log reviews are performed ad hoc based on any suspicious behavior or events that may require further investigation. TAX retains system and security logs according to NIST standards.*
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** *CSAT course, ROB, Insider Threat Training, and Privacy training course via LearnDOJ.*

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The TAX-OAS system security plan, including administrative and technological controls, is documented in accordance with DOJ guidance, policies and directives. The system exists on a physically secure, environmentally protected, DOJ network protected by firewalls, and is administered by DOJ/TAX contractors. All privileged system administrator functions are

performed by DOJ/TAX federal employees. Non-privileged administrative functions are performed by DOJ/TAX contractors who have the appropriate clearance. Access to the TAX-OAS system is only granted to DOJ/TAX federal employees and fully cleared DOJ/TAX contractors. All DOJ/TAX federal employees and DOJ/TAX contractors are required to sign the same confidentiality agreement and system rules of behavior. Access to specific databases/folders/materials is granted on a need-to-know basis requiring a user account and password. All TAX-OAS accounts are "named user" accounts assigned to a single individual and require PIV authentication. A documented process exists for requesting, granting, and reviewing account activity, and terminating accounts. Test, training, or temporary accounts are not permitted in order to accurately log the individual accessing the information.

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.)

Files managed on the TAX-OAS system may include both federal records and non-records that are associated with a wide-array of litigation case files, as well as other administrative and managerial records. The retention policies depend on what type of item it is, whether it is a record, and if so, whether it is required to be maintained as a permanent record. The DOJ record retention schedules are published at Archives.gov (https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-justice/rg-0060). Pursuant to those schedules, TAX litigation case files are currently required to be held for 15 years. Temporary records are then destroyed at the end of the retention period, and permanent records are transferred to the custody of NARA. Paper and electronic non-records are destroyed when no longer needed. Other TAX records have other retention policies, including administrative items on NARA's General Records Schedules.

In accordance with the Federal Records Act, DOJ's Office of Records Management Policy (ORMP), and consistent with NARA standards, TAX ensures that all applications hosted on the TAX-OAS system are in compliance with appropriate retention schedules to manage the use, maintenance, retention, and disposition of DOJ records created and captured.

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:

TAX needs to amend its SORNs Justice/TAX 001 and Justice/TAX 002 to reflect new capabilities and upgrades to some portions of TAX-OAS, however in the meantime, the SORN's listed below cover the applications within TAX-OAS:

- Document Management System
  - Justice/TAX-001*, Criminal Tax Case Files, Special Project Files, Docket Cards, and Associated Records, 71 FR 44 (March 7, 2006) (as amended). See, https://www.govinfo.gov/content/pkg/FR-2006-03-07/pdf/E6-3149.pdf*
  - DOJ-016, *Debt Collection Enforcement System*, (February 21, 2012) (as amended). *See*, https://www.govinfo.gov/content/pkg/FR-2012-02-21/pdf/2012-3913.pdf
  - DOJ-017, *Department of Justice, Giglio Information Files* (March 26, 2015) (as amended). *See https://www.govinfo.gov/content/pkg/FR-2015-03-26/pdf/2015-06934.pdf*
  - Justice/TAX-002*, Civil Tax Case Files, Docket Cards, and Associated Records,* 71 FR 44 (March 7, 2006) (as amended). *See, https://www.govinfo.gov/content/pkg/FR-2006-03-07/pdf/E6-3149.pdf*
  - Justice/Tax-003, *Files of Applications for Attorney and Non-Attorney Positions with the Tax Division,* 71 FR 44 (March 7, 2006) (as amended). *See, https://www.govinfo.gov/content/pkg/FR-2006-03-07/pdf/E6-3149.pdf*
- TaxDoc
  - Justice/TAX-001, *Criminal Tax Case Files, Special Project Files, Docket Cards, and Associated Records,* 71 FR 44 (March 7, 2006) (as amended). *See*, https://www.govinfo.gov/content/pkg/FR-2006-03-07/pdf/E6-3149.pdf
  - Justice/TAX-002*, Civil Tax Case Files, Docket Cards, and Associated Records,* 71 FR 44 (March 7, 2006) (as amended). *See, https://www.govinfo.gov/content/pkg/FR-2006-03-07/pdf/E6-3149.pdf*
  - DOJ-004, *Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records,* 77 FR 26580 (May 4, 2020) as amended). *See*, https://www.govinfo.gov/content/pkg/FR-2012-05-04/pdf/2012-10740.pdf
  - *DOJ-017, Department of Justice, Giglio Information Files (March 26, 2015) (as amended). See https://www.govinfo.gov/content/pkg/FR-2015-03-26/pdf/2015-06934.pdf*
- Human Resources System/Personnel records and files:
  - Justice/Tax-003, *Files of Applications for Attorney and Non-Attorney Positions with the Tax Division,* 71 FR 44 (March 7, 2006) (as amended). *See, https://www.govinfo.gov/content/pkg/FR-2006-03-07/pdf/E6-3149.pdf*

- OPM/GOVT-1, *General Personnel Records*, 71 FR 35347 (December 11, 2020) (as amended). *See*, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf

- OPM/GOVT-2, *Employee Performance File System Records,* 71 FR 35347 (June 19, 2006) (as amended). *See*, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-2-employee-performance-file-system-records.pdf

- DOJ-001, *Accounting Systems for the Department of Justice*, 69 FR 31406 (June 3, 2004) (as amended), *See*, https://www.govinfo.gov/content/pkg/FR-2004-06-03/pdf/04-12578.pdf

- DOJ-006, *Personnel Investigation and Security Clearance Records for the Department of Justice,* (September 24, 2002) (as amended). *See,* https://www.govinfo.gov/content/pkg/FR-2002-09-24/pdf/02-24206.pdf

- DOJ-009, *Emergency Contact Systems for the Department of Justice*, 69 FR 1762 (January 12, 2004) (as amended). *See*, https://www.govinfo.gov/content/pkg/FR-2004-01-12/pdf/04-583.pdf

- DOJ-014, *Department of Justice Employee Directory Systems*, 74 FR 57194 (November 4, 2009) (as amended). *See* https://www.govinfo.gov/content/pkg/FR-2009-11-04/pdf/E9-26526.pdf

- DOJ-011, *Access Control System (ACS)*, 69 FR 232 (December 3, 2004) (as amended). *See*, https://www.govinfo.gov/content/pkg/FR-2004-12-03/pdf/04-26590.pdf

- Automated Litigation Management (E-discovery and FOIA processing)
  - Justice/TAX-001, *Criminal Tax Case Files, Special Project Files, Docket Cards, and Associated Records,* 71 FR 44 (March 7, 2006) (as amended). *See*, https://www.govinfo.gov/content/pkg/FR-2006-03-07/pdf/E6-3149.pdf

  - Justice/TAX-002*, Civil Tax Case Files, Docket Cards, and Associated Records,* 71 FR 44 (March 7, 2006) (as amended). *See, https://www.govinfo.gov/content/pkg/FR-2006-03-07/pdf/E6-3149.pdf*

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 Information Collection

Collecting and maintaining more personal information than necessary to accomplish DOJ's official duties is always a potential threat to privacy. Additional risks to privacy are inherent when the personal data is particularly sensitive, such as a social security number (SSN) or tax identification number, and the potential threat it that the information is not maintained securely. For example, the Internal Revenue Service furnishes TAX with a large amount of confidential and sensitive information of taxpayers, such as taxpayer returns and return information (as defined by 26 U.S.C. § 6103), which includes PII, for TAX's use in its civil litigation and criminal enforcement duties. Return information is broad and includes sensitive income, accounting, and financial data. Furthermore, in conjunction with their work, TAX employees collect additional sensitive income, accounting, and financial data (not return information) in conjunction with its litigation matters.

TAX mitigates this risk by only collecting the data that is required to complete the authorized and necessary functions of TAX. Additionally, TAX mitigates risks to confidentiality through the implementation of data access controls to TAX-OAS, ensuring that information is provided only to those individuals who require access to perform their official duties. Furthermore, information is given only to those individuals who require access to perform official duties. There are no outside users who are permitted access to the TAX-OAS system, including personnel from the larger DOJ community. When a TAX employee departs from TAX, TAX takes appropriate measures to deactivate the user access and accounts to TAX specific information.

Access to SSNs is restricted and only available to certain users with a need to know, for administrative purposes. SSNs stored in TAX-OAS applications are encrypted, and TAX continues to seek alternative methods to avoid and/or minimize the use of SSNs.

b. Potential Threats Related to Use of the Information

Potential threats to privacy as a result of the Department's use of the information in the TAX-OAS system include the risks of unauthorized access to the information, threats to the integrity of the information resulting from unauthorized access or improper disposal of information, and unauthorized disclosure of the information.

TAX primarily mitigates the risks to the sensitive information in its possession by ensuring that access to information is given only to those who require it in order to perform their official duties. Therefore, the primary form of restricting or limiting access to information is by means of access controls, in conjunction with DOJ Identity Management solutions. With information pertaining to civil and criminal cases or matters, access controls restrict permissions to only those TAX employees assigned to a specific case or matter. With non-case information, access controls limit permissions to just that user, and can then be granted to other personnel on a need-to-know basis. There are no outside users who are permitted access to the TAX-OAS system, including personnel from the larger DOJ community. When TAX employees depart, the procedures to terminate access to the TAX-OAS system are promptly implemented by the TAX help desk (TAXI) and the Justice Management Division (JMD) Office of the Chief Information Officer (OCIO). As roles change or users move to new TAX teams, accesses are adjusted and removed to reflect the changes in roles and responsibilities. Usage patterns are tracked and reviewed for anomalous behavior.

On a Department-wide level, TAX's security defenses are shared with DOJ Justice Security Operations Center (JSOC) to ensure appropriate perimeter control and data content monitoring. TAX improves the security defenses by solutions it deploys within the TAX-OAS system, including additional firewalls and monitoring tools.

TAX mitigates risk by limiting access to SSNs. Access to SSNs is restricted and only available to users with a need to know, for administrative purposes. SSNs stored in TAX-OAS applications are encrypted, and TAX continues to seek alternative methods to avoid and/or minimize the use of SSNs. Furthermore, TAX employs a Data Loss Prevention application which prevents SSNs from being emailed outside of TAX.

TAX also mitigates risk by requiring all TAX employees to be adequately trained on their security obligations. TAX employees are required to review and acknowledge Rules of Behavior before being granted access to TAX-OAS. Additionally, all employees are required to complete annual training: the DOJ Cybersecurity Awareness Training (CSAT), specialized training on the restrictions associated with handling taxpayer returns and return information (and, where appropriate, Grand Jury information under Fed. R. Crim. P. 6e), and the DOJ OPCL Privacy Training. Users are often reminded to use care when communicating with employees from other Government agencies, outside counsel, opposing parties, and expert witnesses.

c. Potential Threats Related to Dissemination

There is a potential risk to privacy that could result from improper access and the potential unauthorized disclosure of the information within the TAX-OAS system. However, security protections that authorize and limit a user's access to information within the system mitigate this risk. TAX mitigates this risk by using the DOJ Identity Management solutions, controlling access to information on a need to know basis and providing adequate training in the proper use of the TAX-OAS. As roles change or users move to new TAX teams, accesses are adjusted and removed to reflect the changes in roles and responsibilities. Usage patterns are tracked and reviewed for anomalous behavior. Users are granted access to only the information applicable to their role. Procedures to terminate access to the TAX-OAS system are promptly implemented – when a TAX employee departs/exits/retires – by TAXI, and the JMD OCIO.

On a Department-wide level, TAX's security defenses are shared with DOJ JSOC to ensure appropriate perimeter control and data content monitoring. TAX improves the security defenses by solutions it deploys within the TAX-OAS system, including additional firewalls, data loss prevention software, and monitoring tools.

Appendix A
Privacy Impact Assessment of the Tax Division

The following is an overview of the systems and applications hosted on the TAX-OAS system.

Name	Description
Microsoft Active Directory	The Active Directory system supporting the TAX-OAS is a critical infrastructure that enables all TAX-OAS applications to find services (via DNS) and provide user identification and authentication. Due to its criticality, the architecture for Active Directory is highly distributed and fault-tolerant, with each TAX site having a complete and consistent copy of the Active Directory database. Additionally, the directory service clients are configured to refer to off-site Active Directory servers if the local server fails.
Human Resources System (HRS)	The HRS is a database comprised of several interrelated modules providing workload management primarily pertaining to TAX's employees and contractors. The HRS has reporting capabilities available to the appropriate administrative and management staff of TAX.
TaxDoc	TaxDoc is a database also comprised of several interrelated modules. TaxDoc is TAX's primary case management system, which maintains record of all civil and criminal enforcement matters TAX has received beginning in 1978 or pending as of 1978. TaxDoc supports the application managing case and matter status, summary, assignment, and cross-referencing information. TaxDoc's other applications/modules include: (1) time-keeping of attorneys and other staff, and (2) tracking, through a module, of the FOIA requests TAX receives and processes. TaxDoc has reporting capabilities available to the appropriate TAX administrative and management staff.
Interwoven (iManage) Document Management System (DMS).	TAX's DMS is an electronic records repository consisting of workspaces for TAX's legal, administrative, and management operations. Most of the documents saved in the DMS are created using the suite of Microsoft products: Outlook for email, Word for word processing, Excel for spreadsheets; PowerPoint for presentations. Other documents in the DMS are in .pdf format, created or accessed via Adobe Acrobat. Users access the DMS through the Interwoven client (FileSite) integrated with their Outlook client. The FileSite client communicates exclusively with the Interwoven WorkSite server processes for all DMS functions. WorkSite

	provides an "information broker" service (business logic) on behalf of the client, performing storage, retrieval, and indexing functions.
Automated Litigation Management	The Automated Litigation Support group manages an integrated suite of tools to facilitate automated review of documents in support of TAX's E-Discovery and FOIA processing duties. Internal TAX employees, including contractors, consist of the sole users-base having role-based access to applications residing on the TAX-OAS. One exception to the lone-access is a specific application TAX uses as part of the electronic discovery management process. Access to the electronic discovery application has a specific role-based purpose, with access granted via secure public-facing authentication. DOJ employees, partnering government agency personnel, non-government affiliated expert witnesses/consultants, and other stakeholders in discovery in the court cases and matters TAX handles pursuant to its mission. Moreover, the FOIA personnel use the suite of tools to review and organize records processed in response to FOIA request TAX receives.
TaxNet IntraNet	TaxNet is a repository of logistic resources for employees, including administrative and computer services, civil and criminal litigation, and human resources. TaxNet is a collection of web content hosted on a JCON application server running Internet Information Services (IIS). The TaxNet content is a combination of active and static web pages, with hooks to the document management system.
Annual Bar Membership Submission (ABMS)	The ABMS is an application to assist TAX in complying with the Department's requirement that its attorneys recertify their active membership to a bar and provide proof of active membership. The data the attorneys enter into ABMS is saved in the HRS database. The membership documents uploaded and submitted are saved on a shared drive. The information is collected in a web application that was developed in ASP.NET and is maintained on the web server.