# Office of Justice Programs

**Privacy Impact Assessment**
for the
Discovery for OJP (DISCO)

Issued by:
Maureen Henneberg

Approved by: Katherine Harman-Stokes
Director (Acting), Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: February 2, 2023

*(May 2019 DOJ PIA Template)*

## Section 1: Executive Summary

Discovery for OJP (DISCO) is an automated litigation support tool, that allows OJP's Office of the General Counsel to: collect and preserve; process, review, and analyze; and produce and finally present electronic discovery material in connection with the Department's investigative and litigation functions.

The DISCO system achieves its purpose by making use of a Commercial Off-The-Shelf System (COTS) application (i.e. Relativity) which collects, indexes, and presents documents for attorneys and staff to review as part of an investigation and/or litigation team. The system at its core contains an indexed SQL database which maintains "meta" information about a specific case and the documents being reviewed for that case. It uses web servers to preserve and distribute data, review full text documents, and search concept clusters. Additionally, it can function to search, analyze, and image servers, indexers and processors. All of these tools combine in a web browser interface to give litigation professionals a single cohesive tool in which to perform document review and preparation.

OJP has prepared a Privacy Impact Assessment for DISCO because this system collects, maintains, and disseminates information in identifiable form about individuals mentioned in litigation documents as well as DOJ employees and contractors. Due to the varied nature of the documents ingested by the DISCO system as a part of the litigation process, it is not possible to list with certainty every type of information that will be collected, maintained, or disseminated.

## 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.***

DISCO imports/ingests documentation in a variety of file formats such as Adobe, Microsoft Office suite including Outlook files, and zip applications and allows users to file/review/search through those documents and associated meta-data

The system allows for the ingestion (loading) and dissemination (productions and exports) of material – both unprocessed and processed. Unprocessed material is raw data from the source that provides information to OJP (*e.g.*, another agency, a seized hard drive, etc.) Processed means that OJP has ingested the data and reviewed and updated it. The mechanism for ingesting the data is to place the electronic documents on the OJP servers network disk storage and to instruct the system (through supplied applications) to ingest the documents into a specific (segregated) area for the particular case. The ability to add material to the system is a specific controlled and limited user role. For the dissemination of material, the process is reversed. The system can be instructed (through supplied applications) to export material for review to a specific (segregated) area for the particular case. The ability to export material from the system is also a controlled and limited user role.

DISCO maintains information collected in the course of OJP's investigations and litigation. The information may be collected as part of a client-agency's investigation and provided to OJP or may be produced to OJP by an opposing party in the course of the discovery process. This material could include any and all of the following: federal records, participant and custodian's email, word processor documents, spread sheets, scientific findings, research reports and memoranda, depositions, transcripts of discussion and recording, audio files, video files, image files, multimedia presentations, PowerPoint presentations, personal notes, letters and correspondence. Publicly available information may also be incorporated if deemed relevant to the litigation. Publicly available information may include, but is not limited to, newspaper articles and other published journalism, public records, court records, social media information, and other data traditionally considered "open source." This material is used in the document discovery process of litigation and is only disclosed and distributed as prescribed and overseen by the court.

***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 | 34 USC § 10102; 28 USC § 530C |
| | Executive Order | |
| | Federal Regulation | |
| | Agreement, memorandum of understanding, or other documented arrangement | |
| | Other (summarize and provide copy of relevant portion) | |

## Section 3: Information in the Information Technology

***3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether 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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Name** | X | A, B, C and D | Names of DOJ users and individuals mentioned in litigation materials. |
| **Date of birth or age** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Place of birth** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Gender** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Race, ethnicity or citizenship** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Religion** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Social Security Number (full, last 4 digits or otherwise truncated)** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Tax Identification Number (TIN)** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Driver's license** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Alien registration number** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Passport number** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Mother's maiden name** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Vehicle identifiers** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Personal mailing address** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Personal e-mail address** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Personal phone number** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Medical records number** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Medical notes or other medical or health information** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Financial account information** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Applicant information** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Education records** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Military status or other information** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Employment status, history, or similar information** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Employment performance ratings or other performance information, e.g., performance improvement plan** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Certificates** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Legal documents** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Device identifiers, e.g., mobile devices** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Web uniform resource locator(s)** | X | A, B, C and D | URL based on how the system functions and ingests data, this could potentially be included. |
| **Foreign activities** | | | |
| **Criminal records information, e.g., criminal history, arrests, criminal charges** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Juvenile criminal records information** | | | |
| **Civil law enforcement information, e.g., allegations of civil law violations** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Whistleblower, e.g., tip, complaint or referral** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Grand jury information** | | | |
| **Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information** | | | |
| **Procurement/contracting records** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Proprietary or business information** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| **Location information, including continuous or intermittent location tracking capabilities** | | | |

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| ***Biometric data:*** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| - **Photographs or photographic identifiers** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| - **Video containing biometric data** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| - **Fingerprints** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| - **Palm prints** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| - **Iris image** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| - **Dental profile** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| - **Voice recording/signatures** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| - **Scars, marks, tattoos** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| - **Vascular scan, e.g., palm or finger vein biometric data** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| - **DNA profiles** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |
| - **Other (specify)** | X | A, B, C and D | Based on how the system functions and ingests data, this could potentially be included. |

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| ***System admin/audit data:*** | X | A, B, C and D | Collected from DOJ users. Potentially included in litigation materials. |
| - **User ID** | X | A, B, C and D | Collected from DOJ users. Potentially included in litigation materials. |
| - **User passwords/codes** | X | A, B, C and D | Collected from DOJ users. Potentially included in litigation materials. |
| - **IP address** | X | A, B, C and D | Collected from DOJ users. Potentially included in litigation materials. |
| - **Date/time of access** | X | A, B, C and D | Collected from DOJ users. Potentially included in litigation materials. |
| - **Queries run** | X | A, B, C and D | Collected from DOJ users. Potentially included in litigation materials. |
| - **Content of files accessed/reviewed** | X | A, B, C and D | Collected from DOJ users. Potentially included in litigation materials. |
| - **Contents of files** | X | A, B, C and D | Collected from DOJ users. Potentially included in litigation materials. |
| **Other (please list the type of info and describe as completely as possible):** | X | A, B, C and D | Due to the varied nature of the materials ingested by the DISCO system as a part of the litigation process, it may include categories of information not listed in this table. |

### *3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)*

| **Directly from the individual to whom the information pertains:** | | | | | |
|---|---|---|---|---|---|
| In person | | Hard copy: mail/fax | | Online | |
| Phone | | Email | | | |
| Other (specify): | | | | | |

| **Government sources:** | | | | | |
|---|---|---|---|---|---|
| Within the Component | X | Other DOJ Components | X | Online | 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) | | | |
| Other (specify): | | | | | |

| **Non-government sources:** | | | | | |
|---|---|---|---|---|---|
| Members of the public | | Public media, Internet | X | Private sector | |
| Commercial data brokers | | | | | |
| Other (specify): Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation and investigation purposes. | | | | | |

## Section 4: Information Sharing

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

| **Recipient** | **How information will be shared** | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| Within the Component | X | X | X | OJP's OGC will have access to the system to retrieve user data directly from the system either in bulk or on a case-by-case scenario. |
| DOJ Components | X | | | As necessary in response to active litigation |
| Federal entities | X | | | As necessary in response to active litigation |
| State, local, tribal gov't entities | X | | | As necessary in response to active litigation |
| Public | X | | | Information in a particular matter may become public in accordance with the rules of the tribunal presiding over the litigation matter. |

| 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 | | | As necessary in response to active litigation |
| Private sector | | | | |
| Foreign governments | | | | |
| 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.***

The personally identifiable data within DISCO will not be released to the public for "Open Data" purposes.

## Section 5: Notice, Consent, Access, and Amendment

***5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.***

The Systems of Record Notices listed in section 7.2 provide generalized notice to the public and Privacy Act § 552a(e)(3) notices are provided as needed at the point of collection from individuals. However, there is no secondary notice provided to individuals when the information is loaded in DISCO.

Documents are obtained through requests made to OJP component agencies or individual staff members in their official capacities, or through court order, warrant, subpoena, discovery requests, and other such methods. Individuals do not directly provide information to this system; rather, information about individuals may be contained in documents collected from opposing parties and client agencies in the course of litigation. For social media captures and web site collections, notice is not provided to individuals as the information collected is in the public domain.

***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.***

Individuals do not have the opportunity to decline to provide information. Documents are obtained through requests made to OJP component agencies or individual staff members in their official capacities, or through court order, warrant, subpoena, discovery requests, 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 DISCO. For social media captures and web site collections, notice is not provided to individuals as the information is considered to be in the public domain.

***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 will need to follow the procedures outlined in the applicable SORN for the source records to gain access, request amendment or correction, and receive notification of these procedures. In general, this process would require a written request clearly marked as "Privacy Act Access Request" and addressed to the OJP FOIA Officer, Office of Justice Programs, Office of the General Counsel, 810 7th Street NW, Rm. 5400, Washington, DC 20531. The request must describe the records sought in sufficient detail to enable DOJ personnel to locate them with a reasonable amount of effort. The request should include the requester's full name, current address, date and place of birth, and must be signed and either notarized or submitted under penalty of perjury.

## 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):**<br><br>An ATO was issued on December 16, 2022, and has been authorized until December 22, 2025. |

| | |
|---|---|
| | **If an ATO has not been completed, but is underway, provide status or expected completion date:**<br><br>**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:**<br><br>There are no current active POA&Ms. |
| | **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:**<br>DOJ/OJP Cybersecurity Standards and Continuous Monitoring: DOJ's annual Core Control assessment includes the testing and evaluation of the security and privacy controls safeguarding DISCO information.<br><br>In addition, DOJ/OJP monitors the monthly continuous monitoring submissions from Cloud Service Providers (CSPs) for all Cloud Service Offerings (CSOs) supporting the DISCO system in accordance with the Federal Risk and Authorization Management Program (FedRAMP) Continuous Monitoring 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:**<br>Application audit logs are ingested by Splunk and reviewed in accordance with OJP OCIO 62 Security and Privacy Assessment and Authorization Standard Operating Procedures. |
| 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**. |
| | **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:**<br>There is no additional privacy-related training for this system. |

***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?***

DISCO utilizes role-based access privileges to limit user access. Access to DISCO is granted only to OJP-approved individuals who have signed a confidentiality agreement and system

rules of behavior. Access to specific databases/folders/material is granted on a need-to-know basis by user account and password. All DISCO accounts are "named user" accounts assigned to a single individual.

***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.)***

Information from significant or precedential cases will be permanent, and all other case files will be destroyed 1 year after the end of the fiscal year in which the case is resolved, in accordance with the OJP Records Management Handbook, Series Number 502-02.

## 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:***

The information processed in DISCO could come from any of OJP's systems and are covered by various SORNs, which may include, but are not limited to:

OJP SORNS:

- JUSTICE/OJP-004, Grants Management Information System, last published in full at 53 Fed. Reg. 40526 (Oct. 17, 1988);
- JUSTICE/OJP-008, Civil Rights Investigative System, last published in full at 53 Fed. Reg. 40528 (Oct. 17, 1988);
- JUSTICE/OJP-012, Public Safety Officers Benefit System, last published in full at 84 Fed. Reg. 53749 (Oct. 8, 2019);
- JUSTICE/OJP-013, Denial of Federal Benefits Clearinghouse System, (DEBAR), last published in full at 64 Fed. Reg. 25071 (May 10, 1999);
- JUSTICE/OJP-014, Victims of International Terrorism Expense Reimbursement Program, last published in full at 71 Fed. Reg. 44709 (Aug. 7, 2006);
- JUSTICE/OJP-015, National Missing and Unidentified Persons System, last published in full at 83 Fed. Reg. 13306 (Mar. 28, 2018);
- JUSTICE/OJP-016, Justice Grants System (JustGrants), last published in full at 85 Fed. Reg. 81517 (Dec. 16, 2020);

DOJ-wide SORNs:

- JUSTICE/DOJ-001, Accounting Systems for the Department of Justice, last published in full at 69 Fed. Reg. 31406 (Jun. 3, 2004);
- JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed Reg. 37188 (Jul. 14, 2021);
- JUSTICE/DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (Jun. 4, 2001);
- JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, Mandatory Declassification Review Records, last published in full at: 77 Fed. Reg. 26580 (May 4, 2012);

Government-wide SORNs:

- OPM/GOVT-1, General Personnel Records, last published in full at 77 Fed. Reg. 79694 (Dec. 11, 2012);
- OPM/GOVT-2, Employee Performance File System Records, last published in full at 71 Fed. Reg. 35347 (Jun. 19, 2006);
- OPM/GOVT-3, Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers, last published in full at 71 Fed. Reg. 35350 (Jun. 19, 2006);
- OPM/GOVT-5, Recruiting, Examining, and Placement Records, last published in full at 79 Fed. Reg. 16834 (Mar. 26, 2014);
- EEOC/GOVT-1, Equal Employment Opportunity in the Federal Government Complaint and Appeals Records, last published in full at 67 Fed. Reg. 49338 (Jul. 30, 2002).

## Section 8: Privacy Risks and Mitigation

***When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?***

***Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:***

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
    - The information contained and managed on DISCO is provided to the OJP in the course of litigation or an investigation. Data is collected pursuant to the applicable rules of the tribunal presiding over the litigation. Documents are typically provided by internal OJP entities involved in the investigation or by the opposing party in the litigation in response to a subpoena or other discovery request. The privacy risks associated with

collecting records from other entities is that they will share information outside the scope of the investigation or not properly identify the data being ingested into the system as containing personally identifying information. Preventing the exposure of the data once it is received by the OJP minimizes the risk that personal information will be shared outside the team of individuals working on a particular matter. To this end, the OJP places strict access controls on DISCO via physical and electronic means in order to secure the information.

- The potential compromise of PII in the system is also a risk. To address that concern, the OJP places strict access controls on DISCO via physical and electronic means in order to secure the information. For example, OJP employees and contractors are only granted access to databases on the system that support a matter they are working on. If an employee or contractor leaves or is reassigned, the account access is disabled or access to a particular database may be rescinded. If significant PII is collected incidentally during litigation discovery and production, access to those particular data collections may be further restricted to selected individuals among the case litigation team.

- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***
  - OJP OCIO's IT Security Division (ITSD) is responsible for decisions concerning security and privacy controls. The Information System Security Officer (ISSO) would work with the Information System Security Manager (ISSM), System Owner and Chief Information Security Officer (CISO) in regards to the implementation of technical and physical privacy controls. In addition, ITSD would work with other departments such as Office of the General Counsel (OGC) for the deployment and modification of these privacy controls.
  - Access to information in this system will be restricted to cleared DOJ/OJP personnel accounts. These accounts will use a DOJ network account, email address, and use two-factor authentication to access. Additionally, access to information will be kept on a need-to-know basis with cleared DOJ/OJP personnel.
  - Data is encrypted at rest and in transit and security controls have been implemented in accordance with Section 6 above. DISCO uses FedRAMP which acts as the standard for security assessment and authorization process for cloud products and services used by U.S. Federal agencies.
  - In accordance with DOJ policies and procedures, all DOJ/OJP Federal and Contractor users with access to DOJ networks must complete an annual Cyber Security Assessment Training (CSAT) which includes information on Federal information privacy laws and the requirements for handling PII. Additionally, all DOJ/OJP must sign the DOJ Rules of Behavior as an agreement to confirm they have completed the course and that they agree to abide by the requirements.