

# Justice Management Division (JMD)



## **Privacy Impact Assessment for the JMD ServiceNow**

Issued by:

**Paul Connolly, General Counsel  
Office of the General Counsel  
Senior Component Official for Privacy**

Approved by: Jay Sinha  
Senior Counsel  
Office of Privacy and Civil Liberties  
U.S. Department of Justice

Date approved: August 14, 2026

*(March 2025 DOJ PIA Template)*

## **Section 1: Executive Summary**

ServiceNow is a cloud-based workflow automation platform that enables enterprise organizations to improve operational efficiencies by streamlining and automating routine work tasks and integrating systems to collect, transform, communicate, and return data. The system facilitates workflows and interacts with other systems across DOJ to provide the end-users a one-stop shop to initiate and manage organizational tasks. The system interfaces with IamDOJ (SailPoint)<sup>1</sup> and SharePoint repositories to present a single view of a DOJ personnel which will include information on individual (Name, Email) their organization, the position, and other attributes to include completed training assets assigned, and on-boarding forms completed. The system leverages Okta<sup>2</sup> for authentication and has role-based permissions limiting access to data and workflows based on the user's role.

## **Section 2: Purpose and Use of the Information Technology**

The JMD Services ServiceNow (SN) platform provides a centralized system to enable collaborative work across Human Resources, Budget, and OCIO. It achieves this by aggregating DOJ personnel data and enabling workflows for common employee actions, such as submitting IT-related requests and managing HR processes like on-boarding and off-boarding. This functionality will serve to streamline common requests and workflows to improve operational efficiency, reduce duplication, and leverage current data.

In addition to manual entry, the system integrates with IamDOJ (SailPoint) and SharePoint repositories, which leverage initial personnel data from sources including the National Finance Center (NFC) and Active Directory. ServiceNow presents a single view of DOJ employees and contractors, which will include information on individuals, (name, email) their organization, their position, and other attributes to include training completed, assets assigned, and on-boarding forms completed. ServiceNow uses Okta for authentication and has role-based permissions to limit access to data and workflows based on the user's role and organization. Data within ServiceNow is hosted in the FedRAMP Government Community Cloud (GCC) managed by the vendor and is retained for a minimum of 10 years and may be kept longer for interactions related to capstone users.

### ***2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)***

| <b>Authority</b> | <b>Citation/Reference</b>                                                                        |
|------------------|--------------------------------------------------------------------------------------------------|
| Statute          | E-Government Act of 2002, Public Law 107-347<br>44 USC 3101 – Records management by agency heads |

---

<sup>1</sup> IamDOJ is covered under separate privacy documentation here:

<https://www.justice.gov/opcl/media/1330781/dl?inline>.

<sup>2</sup> Okta is covered under separate privacy documentation here:

<https://www.justice.gov/opcl/media/1347416/dl?inline>.

Department of Justice Privacy Impact Assessment  
**Justice Management Division/JMD ServiceNow**

|                                                                         |                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Executive Order                                                         |                                                                                                                                                                                                                                                                                 |
| Federal regulation                                                      | Federal Information Security Modernization Act of 2014 (FISMA)<br>Federal Information Technology Acquisition Reform Act of 2014 (FITARA)                                                                                                                                        |
| Department order or policy                                              | DOJ Order 0904, Cybersecurity Program (November 2023)<br>DOJ Order 0908, Use and Monitoring of DOJ Information Technology, Information Systems, and Access to Authorized Users' Electronic Information<br>DOJ Security and Privacy Assessment and Authorization (SPAA) Handbook |
| 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.*

The system contains information on Information Technology, Security, Human Resources requests and workflows within JMD. JMD services multiple other components which may have access to the ServiceNow system for their own use cases.

The data includes basic user profile information (name, email, office location, forwarding address (for IT tasks like generating a label for shipping or returning a laptop, position name/title within organization). Additionally, data related to service requests is captured. This includes information related to the requests (asset information like model and barcode) and the nature of the user's issue or request (which may involve textual descriptions and uploaded documentation such as screenshots). The system is used for HR workflows, such as the annual work agreement, where a user may indicate if their request is related to a reasonable accommodation, but no details on the reasonable accommodation are collected, and no other disability or medical accommodation data is collected. The system is used for HR workflows, such as employee onboarding, that collect whether a security clearance briefing is required, but no information on the security level itself is collected. The same HR workflows collect information on pay grade and series, but no other financial information is collected.

Department of Justice Privacy Impact Assessment  
Justice Management Division/JMD ServiceNow

| (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 Detainees;<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                                                                                          |
|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <i>Example: Personal email address</i>                                                              | X                                                                                                                                               | B, C and D                                                                                                                                                                                                                                                      | <i>Email addresses of members of the public (US and non-USPERs)</i>                                   |
| Name                                                                                                | X                                                                                                                                               | A                                                                                                                                                                                                                                                               | Collected as part of employee profile and system interactions.                                        |
| Date of birth or age                                                                                |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Place of birth                                                                                      |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Sex                                                                                                 |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Race, ethnicity, or citizenship                                                                     |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Religion                                                                                            |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Social Security Number (full, last 4 digits or otherwise truncated)                                 |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Tax Identification Number (TIN)                                                                     |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Driver's license                                                                                    |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Alien registration number                                                                           |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Passport number                                                                                     |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Mother's maiden name                                                                                |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Vehicle identifiers                                                                                 |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Personal mailing address                                                                            | X                                                                                                                                               | A                                                                                                                                                                                                                                                               | Personal Mail address is collected for IT equipment shipments and returns.                            |
| Personal e-mail address                                                                             | X                                                                                                                                               | A                                                                                                                                                                                                                                                               | Personal Email is collected for IT equipment shipments and returns.                                   |
| Personal phone number                                                                               | X                                                                                                                                               | A                                                                                                                                                                                                                                                               | Phone number collected for IT equipment shipments and returns.                                        |
| Medical records number                                                                              |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Medical notes or other medical or health information                                                | X                                                                                                                                               | A                                                                                                                                                                                                                                                               | Work agreement may indicate reasonable accommodation (no medical or disability information collected) |
| Financial account information                                                                       |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Applicant information                                                                               |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Education records                                                                                   |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Military status or other information                                                                |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Employment status, history, or similar information                                                  |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Employment performance ratings or other performance information, e.g., performance improvement plan |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |
| Certificates                                                                                        |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                       |

Department of Justice Privacy Impact Assessment  
Justice Management Division/JMD ServiceNow

| (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 |
|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Legal documents                                                                                             |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| Device identifiers, e.g., mobile devices                                                                    |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| Web uniform resource locator(s)                                                                             |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| Foreign activities                                                                                          |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| Criminal records information, e.g., criminal history, arrests, criminal charges                             |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| Juvenile criminal records information                                                                       |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| Civil law enforcement information, e.g., allegations of civil law violations                                |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| Whistleblower, e.g., tip, complaint, or referral                                                            |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| Grand jury information                                                                                      |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| Procurement/contracting records                                                                             |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| Proprietary or business information                                                                         |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| Location information, including continuous or intermittent location tracking capabilities                   |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| <i>Biometric data:</i>                                                                                      |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| - Photographs or photographic identifiers                                                                   |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| - Video containing biometric data                                                                           |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| - Fingerprints                                                                                              |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| - Palm prints                                                                                               |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| - Iris image                                                                                                |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| - Dental profile                                                                                            |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| - Voice recording/signatures                                                                                |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| - Scars, marks, tattoos                                                                                     |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| - Vascular scan, e.g., palm or finger vein biometric data                                                   |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| - DNA profiles                                                                                              |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |
| - Other (specify)                                                                                           |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |              |

Department of Justice Privacy Impact Assessment  
Justice Management Division/JMD ServiceNow

| (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                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>System admin/audit data:</i>                                              |                                                                                                                                                 |                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                          |
| - User ID                                                                    | X                                                                                                                                               | A                                                                                                                                                                                                                                                               | Authentication is handled via DOJ Login. ServiceNow keeps audit trail of user login with ID and date stamp                                                                                                                                                               |
| - User passwords/codes                                                       | X                                                                                                                                               | A                                                                                                                                                                                                                                                               | Authentication is handled via DOJ Login. ServiceNow keeps audit trail of user login with ID and date stamp                                                                                                                                                               |
| - IP address                                                                 | X                                                                                                                                               | A                                                                                                                                                                                                                                                               | Authentication is handled via DOJ Login. ServiceNow keeps audit trail of user login with ID and date stamp                                                                                                                                                               |
| - Date/time of access                                                        | X                                                                                                                                               | A                                                                                                                                                                                                                                                               | Authentication is handled via DOJ Login. ServiceNow keeps audit trail of user login with ID and date stamp                                                                                                                                                               |
| - Queries run                                                                | X                                                                                                                                               | A                                                                                                                                                                                                                                                               | ServiceNow keeps audit trail and user logs of queries run                                                                                                                                                                                                                |
| - Contents of files                                                          | X                                                                                                                                               | A                                                                                                                                                                                                                                                               | ServiceNow keeps audit trail and user logs of contents files.                                                                                                                                                                                                            |
| Other (please list the type of info and describe as completely as possible): | X                                                                                                                                               | A, B, C, D                                                                                                                                                                                                                                                      | Data may include user-submitted screenshots attached to IT or HR requests, which could contain incidental PII. Due to the varied nature of workflows, it is not possible to list with certainty every item of information that may be collected or stored by the system. |

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

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

| Government sources:  |   |                                                                                                                                                  |   |                        |   |
|----------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------|---|------------------------|---|
| Within the Component | x | Other DOJ Components                                                                                                                             | x | Other federal entities | x |
| State, local, tribal |   | 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 |  | Private sector |
| 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                    | Data shared with DOJ employees/contractors. Data is shared via direct login or email communication with personnel on a need-to-know basis. Data is shared to conduct internal business activities, which include IT Service Management, Audit Tracking and HR Service Management. Access is controlled via DOJLogin (Okta) with “least privileged” and “need-to-know” role-based policies applied. Data in-transit and stored data is encrypted. |

Department of Justice Privacy Impact Assessment  
Justice Management Division/JMD ServiceNow

| 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.                                                                                                                                                                                                                                                                                                        |
| DOJ Components                                                                                       | x                              |               | x                    | Data shared with DOJ employees/contractors. Data shared via direct login or email communication with personnel on a need-to-know basis. Data is shared to conduct internal business activities, which includes IT Service Management, Audit Tracking and HR Service Management. Access is controlled via DOJLogin (Okta) with “least privileged” and “need-to-know” role-based policies applied. Data in-transit and stored data is encrypted. |
| Federal entities                                                                                     |                                |               |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| State, local, tribal gov't entities                                                                  |                                |               |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Public                                                                                               |                                |               |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes |                                |               |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 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.*

JMD ServiceNow information will never be released to the public for “Open Data” purposes.

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

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

ServiceNow aggregates information from other source systems and does not collect information directly from individuals. Therefore, notice is provided by the source systems. The applicable System of Records Notices (SORNs) (see Sec. 7.2, below) provide generalized public notice of the collection, use, and sharing of JMD ServiceNow information. No other notice specific to the collection, use, and sharing of the individual's PII is provided.

- 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.*

There is no opportunity for individuals to voluntarily participate in the collection, use, or dissemination of information in the system. Employees and contractors assigned access to Department information and information technology do not have the opportunity to voluntarily participate in the collection, use or dissemination of information in the system. Employees' and contractors' consent to the collection or specific uses of their information by acknowledging the Department's Information Systems Warning Banner is displayed within the DOJ log-in screen each time a user accesses the JMD ServiceNow system.

- 5.3** *What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.*

The Privacy Act permits an individual to gain access to records or any information pertaining to that individual which is contained in a system of records (here, JMD-022), subject to certain limitations and exemptions. The Department processes all Privacy Act requests for access to records under both the Privacy Act and the Freedom of Information Act (FOIA), 5 U.S.C. § 552. The Privacy Act also permits an individual to request an amendment or correction of a record pertaining to that individual, subject to certain limitations and exemptions. A request for amendment or correction of a Department of Justice record can be made by appearing in person or writing directly to the Department component that maintains the record.

## **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).*

Department of Justice Privacy Impact Assessment  
Justice Management Division/JMD ServiceNow

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| X | <p><b>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 the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):</b></p> <p>JMD ServiceNow's ATO was completed on April 26, 2026, and will expire on April 26, 2029.</p> <p><b>If an ATO has not been completed, but is underway, provide status or expected completion date:</b> N/A</p> <p><b>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:</b> N/A</p> |
|   | <p><b>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:</b> N/A – The system has an ATO</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| X | <p><b>This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:</b></p> <p>JMD ServiceNow is categorized as a Moderate-impact system, in accordance with Federal Information Processing Standards (FIPS) 199 – Standards for Security Categorization of Federal Information and Information Systems. To support the FIPS 199 designation of Moderate, the information contained in JMD ServiceNow is categorized as sensitive but unclassified. JMD ServiceNow does not manage high value assets (HVA) as defined by DOJ IT security policy.</p>                                                                                                                    |
| X | <p><b>Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:</b></p> <p>As standard operating procedure, the computer servers supporting this project are built with secure configuration policies such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). Department approved monitoring agents such as IBM Endpoint Lifecycle Management System (ELMS) are deployed to monitor and identify component assets. On a weekly basis, the Department of Justice Privacy Impact Assessment, vulnerability assessments and risk management procedures are executed on operating systems (OS), software applications, and database resources.</p>                                                                                                                                                                                                                                                                                                                                                                                                                       |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| X | <p><b>Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:</b></p> <p>ServiceNow collects audit log data from various components including but not limited to; servers, network devices, appliances, databases and applications, and Ensure that logs are received daily for all appropriate network devices, servers and databases. Conduct log analysis through the log analysis alerts as an integral part of security monitoring. Review privileged user activity to identify any anomalous behavior. Conduct log analysis through both the central log management and analysis solution and local logs in support of security incidents.</p> |
| X | <p><b>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.</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| X | <p><b>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:</b></p> <p>JMD ServiceNow does not provide privacy-related training specific to JMD ServiceNow. Rather, it relies on the foundational privacy-related training included in the Department's annual Computer Security and Awareness Training (CSAT) and General and Privileged rules of behavior (ROB).</p>                                                                                                          |

**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 following information technology and physical controls are in place to reduce the risk of unauthorized access or disclosure of PII:

- Periodic vulnerability assessment activities such as system weakness discovery, and system patch and update deployment are conducted.
- Detailed operating system log management and potential incident analysis activities are performed.
- Intrusion protection/prevention system and anti-virus tools are deployed on system resources.
- Department-level access control lists are deployed with specific controls granted to designated employee or contractor users of the system.
- Access controls such as account authorization, routine account verification, and role-based security controls for user identification (based on role-based policies of "least privileged" and "need-to-know").
- Two-factor authentication prior to system access.
- Encryption of data in-transit and data-at-rest via IT encryption tools.
- Detection of unauthorized access to the system via scheduled account verification and

Department of Justice Privacy Impact Assessment  
**Justice Management Division/JMD ServiceNow**

- review of audit logs and configuration file logs.
- The Department's management of physical access controls based on the user's background investigation category and security level.

**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.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.*

The applicable records disposition schedule states that information in the system shall be destroyed/deleted 15 years after the final disposition of the information

## **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:*

DOJ-014, "Department of Justice Employee Directory Systems," 74 FR 5570 (2-3-2012)\*, 82 FR 24151, 154 (5-25-2017)

DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," [86 FR 37188](#) (7-14-2021)

## **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? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.*

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

Department of Justice Privacy Impact Assessment  
**Justice Management Division/JMD ServiceNow**

- *Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),*
- *Sources of the information,*
- *Type of technology employed (e.g. AI/ML),*
- *Specific uses or sharing,*
- *Privacy notices to individuals, and*
- *Decisions concerning security and privacy administrative, technical, and physical controls over the information.*

JMD ServiceNow (JMD SN) hosts tools, services, and applications that may collect PII, and those systems may collect other sensitive systems operation information to include names, personal e-mail addresses, personal phone numbers, device identifiers, and system admin/audit data (e.g., user IDs, user passwords, IP addresses, date/time of actions, queries run, contents of files).

JMD ServiceNow collection and use of PII, as described here and throughout this PIA, may create certain privacy risks. To mitigate these risks, all data retention is managed according to the National Archives and Records Administration (NARA) requirements and Department associated policies.

JMD ServiceNow does not collect certain data types such as Social Security Numbers and Tax Identification Numbers) from its users, nor from the subjects of an investigation or persons with an interest in the outcome of a case, to minimize the collection of PII.

JMD ServiceNow manages the systems automatically collecting information, and from external government sources such as other Federal Government agencies where applications hosted by JMD ServiceNow are offered as a service. To further mitigate any risks associated with these activities, ServiceNow implements encryption, account management and access controls, auditing, and system monitoring tools to mitigate and protect PII.

JMD ServiceNow has deployed system endpoint protection to detect, stop, or remove malicious software, defend assets against viruses, buffer overflow issues, and prevent malware or hidden files from installing on devices. JMD ServiceNow makes use of separate privileged and non-privileged user accounts and access is granted based on least privilege and need-to-know requirements. DOJ users (government and contractors) are not provided an opportunity to voluntarily participate in the collection, use or dissemination of Department of Justice Privacy Impact Assessment JMD ServiceNow.

JMD ServiceNow System Administrators. Information is shared on a case-by-case basis within the component and other DOJ Components, Information is shared with the private sector via the Freedom of Information Act (FOIA) policy and procedures. Also, for any risks associated with these activities, JMD SN uses encryption and logging controls for mitigation purposes.

The JMD SN ISSO performs continuous monitoring of the security controls within the system to ensure security protections are operating as intended. By Department Order, all DOJ users with access to Department networks, including JMD SN, must receive an annual Cyber Security Assessment Training (CSAT). The CSAT course includes information on certain federal

Department of Justice Privacy Impact Assessment  
**Justice Management Division/JMD ServiceNow**

information privacy laws, such as the Privacy Act, and requirements for proper handling of PII. The course identifies potential risks and vulnerabilities associated with using DOJ-owned IT systems, provides a review of the user's role in protecting these systems, and establishes guidelines to follow at work and in mobile settings to protect against attacks on IT systems. All employees and contractors must also annually sign a DOJ Rules of Behavior agreement confirming that they have completed this course and that they agree to abide by such requirements reviewed in the course.

Failure to successfully complete this training can result in termination of the employee or contractor's access to DOJ computers. Participation in the training course is tracked to ensure that DOJ employees and contractors comply with this training. In conclusion, to ensure the continued relevance and effectiveness of security controls, risk assessments, including privacy and security control assessments are routinely evaluated. In accordance with the NIST Special Publication 800-53 (Rev.5), these assessments include the management, operational, and technical controls to ensure minimization of any privacy risk.