Civil Rights Division

Privacy Impact Assessment
for the
CRT-Service Now Claimant Portal

Issued by:

Kilian B. Kagle
FOIA/Privacy Act Chief
Civil Rights Division
U.S. Department of Justice

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

Date approved: July 22, 2021

(May 2019 DOJ PIA Template)

[This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) at https://www.justice.gov/opcl/file/631431/download.] The following questions are intended to define the scope of the information in the information technology, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the information technology.]

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Department of Justice (DOJ) Civil Rights Division (CRT) is using ServiceNow (SNOW), a FedRAMP High-compliant Software as a Service (SaaS) cloud-hosting provider offering a suite of natively integrated applications designed to support Information Technology Service Management (ITSM), resource management, and shared support services. The CRT is leveraging SNOW for IT services, which include, but are not limited to helpdesk services (IT Ticketing), incident management, change management, knowledge management, configuration management and automated workflows to support employee/contractor onboarding-offboarding. CRT will also be using ServiceNow to provide the Claim Settlement Application, which will be used to process claimant's award settlements in connection with anti-discrimination cases brought by CRT. The Claim Settlement application will collect claimant data used to determine the claimant's eligibility for awards and will support CRT in calculating the award amount.

CRT prepared this Privacy Impact Assessment because ServiceNow will be used to collect, use, and maintain personally identifiable information (PII) about members of the public.

Section 2: Purpose and Use of the Information Technology

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

The purpose of the project is to provide Civil Rights Division users with online E-Request application for helpdesk tickets, knowledge management, and configuration management capabilities.

Through the CRT SNOW online user interface, DOJ users can submit incident tickets, change requests and other requests for IT services or utilize the knowledge management functionality for self-help. All CRT users will access the SNOW SaaS with government furnished equipment. Users validate credentials with two-factor authentication using the Personal Identity Verification (PIV) card, and the system interfaces with Active Directory Federation Services to authenticate users.

CRT's ServiceNow system administrators manage performance issues and incidents with the supported IT infrastructure. CRT-SNOW tracks all incidents and changes via tickets and notifies all involved parties of updates until the incident has been resolved.

SNOW collects some configuration information using auto-discovery and monitoring solution. The information includes, but is not limited to device identifiers, laptops, server hostname, and operating system. CRT also collects information from CRT employees and contractors to support onboarding/offboarding and IT provisioning (User Accounts, System Access, Laptops, iPhones, Office Spaces). The information collected includes first names, last names, email address, phone number, and employment information.

DOJ CRT will also employ ServiceNow's Customer Service Management (CSM) self-service portal functionality to host an external-facing Claimant Portal via the internet. The Claimant Portal will allow claimant organizations and 3rd party claim administrators the option to submit claimant information via the self-service portal. The Claimant Portal objective is to streamline the claimant data entry and claim eligibility determination processes. CRT information is restricted to authorized privileged users (System Administrators).

The CRT Employment Litigation Section (ELS) will be using the claimant information submitted to the Claimant Portal to make eligibility determinations and propose relief distribution. This will require ELS to:

1. Store the existing employment-related data;
2. Store the existing contact information and facilitate the updating of contact information, as needed;
3. Allow for electronic submission of claim forms;
4. Record and import information from claim forms submitted by Claimants;
5. Identify follow-up required to obtain information based on claim forms submitted;
6. Use data from claim forms, employment-related data, and possibly follow-up contacts to evaluate whether Claimants are entitled to individual relief;
7. Use formulas to calculate how much monetary relief to award to each eligible Claimant seeking such relief;
8. Use formulas to calculate Claimant's eligibility for other benefits including vacation days, a hiring bonus, and a specific retroactive seniority date;
9. Prepare lists to file with the Court identifying Claimants entitled to individual relief and back pay award amounts;
10. Prepare spreadsheets to allow the Claims Administrator to populate letters informing each Claimant of the United States' determination regarding whether the Claimant is entitled to the individual relief sought; if eligible for back pay, how much; and if ineligible, the reason(s);
11. Track and organize objections from Claimants (or others) to CRT's relief determinations, and any adjustments made based on those objections;
12. Prepare spreadsheets to facilitate the Claims Administrator's preparation and acceptance of individual relief awards and release of claims forms to inform each Claimant of the Court's determination regarding whether the Claimant is entitled to the individual relief sought; if eligible for back pay, how much; and if ineligible, the reason(s);

13. Track acceptance of relief and release of claims forms submitted by Claimants and any follow-up required to obtain missing information;
14. Track adjustments made to relief based on Acceptance of Relief forms;
15. Update lists identifying Claimants entitled to individual relief and back pay award amounts, based on who submits acceptance of relief and release of claims forms;
16. Track adjustments made to relief based on Claimants' failure to cash checks; and
17. Update lists identifying Claimants' entitlement to back pay award amounts, based on Claimants' failure to cash checks.

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

Authority		Citation/Reference
	Statute	44 U.S.C § 3506, 40 U.S.C. § 11315 and 5 U.S.C. §301
	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: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	B, C, D	Claimant name
Date of birth or age	X	B, C, D	Claimant date of birth
Place of birth	X	B, C, D	Claimant place of birth
Gender	X	B, C, D	Claimant gender
Race, ethnicity or citizenship	X	B, C, D	Claimant race, ethnicity, or citizenship
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	B, C, D	Claimant's full Social Security Number (SSN)
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	B, C, D	Claimant mailing address
Personal e-mail address	X	B, C, D	Claimant email address
Personal phone number	X	B, C, D	Claimant phone number
Medical records number			
Medical notes or other medical or health information			
Financial account information	X	B, C, D	Claimant's tax document(s)
Applicant information			
Education records	X	B, C, D	Claimant education records
Military status or other information	X	B, C, D	Claimant military status
Employment status, history, or similar information	X	B, C, D	Claimant employment information
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	B, C, D	Claimant's felony convictions, expungements
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	B, C, D	Claimant's civil law enforcement matters
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			
Biometric data:			
- **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)**			
System admin/audit data:			
- **User ID**			
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**			
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Other: PII	X	B, C, D	Claimant's recent drug use must be collected in accordance with the terms of CRT's settlement with the Baltimore County Police Department. Claimants may be required to submit other PII elements if required by future settlement agreements.

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): Service Now Claimant Portal					

Government sources:					
Within the Component		Other DOJ Components		Online	
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.

Through the claims process, claimants will submit their personal information to a third party claims administrator (e.g., name, social security number, date of birth, contact info). Information submitted to a claims administrator will then be used to update the information in the DOJ Claim Settlement portal/database.

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	This data will be used by CRT Claim Processors to determine Claimant Settlement eligibility and award.
DOJ Components				
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.

No information from SNOW will be made 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.

CRT will notify individuals directly with a Privacy Act §552a(e)(3) notice for individuals.

General notice has also been given that records maintained for the purpose of vetting and determining an individual's membership in a claimant class, and determining an individual's right to relief based on membership in a claimant class are covered by JUSTICE/CRT-001, "Central Civil Rights Division Index File and Associated Records" 68 FR 47610, 611 (August 11, 2003), 70 FR 43904 (July 29, 2005), 82 FR 24147 (May 25, 2017).

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.

Claimant must provide the required PII only if they would like to be considered for Eligibility for Claim settlement.

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.

Through the claim settlement process, claimants will submit their personal information to a third party claims administrator. Information submitted to a claims administrator will then be used to update the information in the DOJ CRT Claim Settlement portal/database. In addition, all potential claimants will be provided a DOJ Civil Rights Division email address and phone number for matters related to their claim including updates and corrections to their PII.

In addition, records maintained for the purpose of vetting and determining an individual's membership in a claimant class, and determining an individual's right to relief based on membership in a claimant class can be accessed or amended, in accordance with DOJ regulations, and in accordance with JUSTICE/CRT-001, "Central Civil Rights Division Index File and Associated Records" 68 FR 47610, 611 (August 11, 2003), 70 FR 43904 (July 29, 2005), 82 FR 24147 (May 25, 2017).

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):** 2/22/2019 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **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:**
	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:**
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:**
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:**

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?

Security controls commensurable to the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publications No. 199, "Standards for Security Categorization of Federal Information and Information Systems[1]", are in place as described in the IT system security plan.

The security controls that protect the privacy of individuals and operations at CRT are set and maintained primarily by domain policy. Domain policy is a set of directions and controls that are stored on the primary authentication servers and are automatically applied to all computers and accounts within the domain. The controls force compliance to security policies to the extent possible.

[1] FIPS Publication No. 199 can be found here: https://csrc.nist.gov/publications/detail/fips/199/final.

The policies are automatically applied to all systems and accounts within the CRT operating unit upon log-on or power-up. The policies are maintained and validated by periodic scanning and system checks. The primary responsible technicians are the Information Systems Staff (ISS) system administrators and service desk personnel.

Access to the system is limited to a need to know. Rules of behavior and non-disclosure agreements for all users are required before network access is provided. Access to the system is safeguarded using two factor authentication. CRT staff also receive annual computer security awareness training regarding how to properly protect PII in accordance with Department of Justice standards.

CRT will utilize the ServiceNow Social Security Masking feature whereby only the last-4 digits of the Claimant's Social Security number will be displayed to users not authorized to access the full SSN.

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.)

Claimant information retained and collected in the database is considered temporary, and thus can be disposed of when the case is closed. The specific retention schedule is in the process of being updated, and will be included in forthcoming records guidance, which likely will be distributed to CRT in the next month or two. The forthcoming guidance indicates that databases should be deleted or destroyed after the case concludes.

Section 7: Privacy Act

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

_____ No. __X___ Yes.

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

JUSTICE/DOJ-002, 64 FR 73585 (Dec. 30, 1999), as modified by 66 FR 8425 (Jan. 31, 2001) and 82 FR 24147 (May 25, 2017) and JUSTICE-CRT-00168 FR 47610, 611 (August 11, 2003), 70 FR 43904 (July 29, 2005), 82 FR 24147 (May 25, 2017).

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),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

In order to limit the risk of overcollection or misuse of information, DOJ CRT will be collecting the minimal PII data types required from a claimant that is required to process a claim. Claimants will submit their personal information to a third-party claims administrator. Information submitted to a claims administrator will then be used to update the information in the DOJ CRT Claim Settlement portal/database.

CRT will be referencing the following verbiage on the Website and Claimant Portal related DOJ CRT compliance with *a Privacy Act § 552a(e)(3) notice for individuals.*

The Claim Settlement Portal/Database will be hosted on the ServiceNow Platform in the FedRAMP High cloud. DOJ CRT will be leveraging the ServiceNow platform security architecture which include a comprehensive list of technical and physical controls to ensure data privacy and protection, including:

- Role-based Access Control: Role-based access control (RBAC) is a method of access security that is based on a person's role within a business. Role-based access control is a way to provide security because it only allows employees to access information they need to do their jobs, while preventing them from accessing additional information that is not relevant to them.

- Access Control Lists (ACLs): An access-control list (ACL) is a list of permissions associated with a system resource (object)**.** An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

- Edge Encryption: Edge Encryption is a network encryption system that resides on your network and that encrypts and decrypts sensitive data as it travels between your data center and the ServiceNow cloud. Edge Encryption complies with FIPS-140-2.[2] Edge Encryption supports standard, equality-preserving, and order-preserving encryption types.

- Data Encryption in transit, rest, and database: Data is encrypted on premises before sending it over the Internet to the ServiceNow instance (encrypted in transit), where it remains encrypted at rest. All stored data in databases is encrypted and individual records or tables are decrypted in memory while being accessed. New or changed data is encrypted as it is entered into a table and associated activity log files (bin, redo, undo, and error) are also encrypted.

[2] FIPS 140-2 can be found at: https://csrc.nist.gov/publications/detail/fips/140/2/final