Antitrust Division

Privacy Impact Assessment
for the use of
ServiceNow ("SNow")

Issued by:
Sarah Oldfield
Senior Component Official for Privacy

Approved by: Michelle Ramsden
Senior Counsel
U.S. Department of Justice

Date approved: December 10, 2024

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 Antitrust Division (ATR) ServiceNow (ATR SNow) is in a Government Community Cloud (GCC) environment that is hosted exclusively within ServiceNow® datacenters. ServiceNow® is a cloud computing platform which helps organizations manage digital workflows for enterprise operations. ATR SNow contains and supports several IT service management capabilities and solutions using the following modules:

- IT Service Management (ITSM) module helps ATR manage its IT infrastructure and services, including incident management, problem management, change management, and asset management.

- Configuration Management Database (CMDB) module helps ATR manage its configuration changes for the ATR infrastructure, including network configuration, firewall changes, vulnerability updates, and group policy updates, using automated workflows.

- Human Resources Service Delivery (HRSD) module streamlines ATR's Human Resources (HR) processes and delivers a better employee experience through advanced employee self-service, HR case management, and onboarding and offboarding support. ATR's HR staff use ServiceNow® to replace manual review of forms and simplify workflow and approval processes. For instance, HR staff use ServiceNow® to manage on-boarding of new employees and contractors, telework requirements, off-boarding procedures, retirement activities, budget requirements, and the flexibility to generate on-demand reports. ATR SNow also allows HR to track official passports issued to ATR personnel, as well as compile and review information obtained through surveys for new and departing employees.

ATR authorized users access the ATR SNow application through a link located on ATR's intranet (ATRNet) using any web browser.

In the future, ATR SNow will be integrated with other ATR systems, namely a matter management system ("Salesforce"), and a document and records management system ("Feith Systems"). ATR may also acquire an additional module, Security Operations ("SecOps"), to simplify and automate threat and vulnerability management and response, reach operational agility, and prioritize remediation, allowing ATR to know its security posture and reduce risk to its environment.

ServiceNow® uses Artificial Intelligence (AI) agents to orchestrate workflows, integrations, and data governance across ATR, as well as for IT and Customer Service, or to create custom agents tailored to the unique needs of ATR. ATR's use of AI in this context improves employee workload and efficiency. The following AI features are included under ATR's ServiceNow® subscription.

For the HRSD Enterprise and the ITSM Professional:

- Predictive Intelligence: a platform function that provides a layer of artificial intelligence to improve the ATR user experience, for instance, by assigning, categorizing, and prioritizing tasks.
- Virtual Agent: a function which enables ATR users to engage with live agents, virtual agents, or both using ServiceNow® Conversational Interfaces.
- AI Search: a function which provides a search engine using intelligent queries for ServiceNow® Service Portal, ServiceNow® Now Mobile, and ServiceNow® Virtual Agent.

At the time ATR selected products for this project, Now Assist (ServiceNow®'s Generative (Gen) AI offering) was not available and, as such, was not included in all of the products that ATR purchased in its subscriptions. For example, Gen AI features are not embedded in existing Pro and Enterprise SKUs, rather, they are packaged in add-on SKUs containing features relevant for each workflow. The two ServiceNow® workflow Business Units ATR is subscribed to that have released Now Assist capabilities are ITSM and HRSD.

ATR SNow imports and exports source data from the following federal entities:

1. Electronic Official Personnel Folder (eOPF): Government staff electronic records (SF50, SF52, and PWP, and benefits forms);
2. National Finance Center (NFC): Government staff payroll and financial data, as well as personal information;
3. USA Hire and Staffing: Potential government staff personal information, vacancy announcement, resume, and offer letter;
4. USA Performance: Government staff performance appraisals and performance plans; and
5. ATR users can input data directly into the ATR SNow application, as needed.

This Privacy Impact Assessment (PIA) was prepared because ATR SNow contains information in identifiable form. This PIA covers, in part, functionality that was once described in the ATR Application Management Suite (ATR AMS) PIA. As required by Section 208 of the E-Government Act of 2002, this PIA explains how such data is stored, managed, and shared, in accordance with Federal privacy and information protection guidelines.

<u>Section 2</u>: 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 Technology Directorate (TD) acquired software licensing and professional services to migrate off a ServiceNow® instance hosted by DOJ Alcohol, Tobacco, and Firearms (ATF), and deployed an ATR-owned-and-operated ServiceNow® instance that includes the following capabilities:

- IT Service Management (ITSM): At the core of TD's day-to-day activities, the ITSM component centralizes and automates service management to increase efficiency, standardize support models, lower costs, and free valuable resources to focus on efforts to improve user experience.
- IT Asset Management (ITAM): The ITAM component provides core asset management capabilities to manage ATR's infrastructure, operations, and field services.
- Integration Hub: The Integration Hub enables integrations including DOJ shared services for asset discovery management and endpoint security, audit and vulnerability management, mobile device management, and secure access authentication and authorization services.

ATR uses ServiceNow® professional services to assist employees and contractors with matters like:

- Software Models;
- Data Capture Fields;
- User Interface Action and Business Rules;
- Workflows;
- Dashboard or Reports;
- Import historical solution data from one (1) legacy source one (1) time; and
- Configure historical solution process steps based on user Stories.

ATR uses ServiceNow® to assist employees and contractors with HR matters like:

- Onboarding;
- Employee Records;
- Hiring Dashboard;
- Benefits;
- Reporting;
- Employee Rewards; and
- Email Notifications.

The ATR SNow HRSD module interfaces with existing applications and tools through API such as:

- National Finance Center (NFC);
- USA Onboarding application;
- USA Staffing application;
- NFC's Employee Personal Page (EPP) system;
- Electronic Official Personnel File (eOPF);
- Custom Export Excel Files (i.e. Inventory of Active, Requested and Completed positions); and
- Employee Rewards (custom spreadsheet that gathers information from different offices for handling employee rewards).

ATR SNow provides communications capability via email for various notifications, including hiring and general communication, and is part of workflow for personnel processes and paperwork alerting managers and supervisors about work plans, etc.

ATR SNow integrates with the WebTA and NFC payroll systems and allows employees access to a self-service portal to engage with performance tools, benefits, time and attendance and other HR functions that were formerly manual. ATR SNow automates processes to reduce dependency on HR staff and allows employees to perform HR specific required tasks. ATR SNow automatically sends out notifications of new tasks and reminders.

Finally, ATR uses ServiceNow® as appropriate to assist employees and contractors with:

- Capturing and reporting full logging of user activity, including deletions;
- Accessing logs and activity reports using industry-standard best practices;
- Conducting logging, log retention, and log management that meets or exceeds the requirements in OMB M-21-31, along with applicable NIST, NARA, DHS CISA, and ATR requirements;
- Meeting federal information processing standard (FIPS) 140-2 or FIPS 140-3 certified cryptomodules for all encryptions;

- Encrypting data at rest and data in transmission while the solution is safeguarding data, including but not limited to user data, application data, network traffic, and authentication;

- Ensuring display of a logon or warning banner with end-user acknowledgment to proceed; and
- Maintaining a cloud-based audit management system hosted by DOJ Shared Services.

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	
Executive Order	
Federal regulation	28 C.F.R. §§ 0.40 and 0.41
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	A, B, C & D	A/B - Database contains human resource data for all employees, including detailees, as downloaded from the National Finance Center. It is maintained by the HR staff. C/D – Outside Experts/Vendors receive Government Furnished Equipment (GFE) to support contract work with ATR.
Date of birth or age	X	A	Database contains human resource data for all employees as downloaded from the National Finance Center. It is maintained by the HR staff.
Place of birth			
Gender	X	A	Database contains human resource data for all employees as downloaded from the National Finance Center. It is maintained by the HR staff.
Race, ethnicity, or citizenship	X	A	Database contains human resource data for all employees as downloaded from the National Finance Center. It is maintained by the HR staff.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A	Social Security numbers are collected in full but are masked in the ServiceNow® database table. Database contains human resource data for all employees as downloaded from the National Finance Center. It is maintained by the HR staff and has very limited controlled use.
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number	X	A	Passport information is stored for staff having a government issued passport. Records can include personal passport book or card numbers. This data is maintained and used by the HR and International Sections.
Mother's maiden name			
Vehicle identifiers			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to:
		A. DOJ/Component Employees, Contractors, and Detailees;
		B. Other Federal Government Personnel;
		C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs);
		D. Members of the Public Non-USPERs
			(4) Comments

Personal mailing address	X	A, B, C & D	A/B - Database contains human resource data for all employees, including detailees, as downloaded from the National Finance Center. It is maintained by the HR staff and has limited controlled use. C/D – Outside Experts/Vendors receive GFE to support contract work with ATR.
Personal e-mail address	X	A, B, C & D	A/B - Database contains human resource data for all employees, including detailees, as downloaded from the National Finance Center. It is maintained by the HR staff and has limited controlled use. C/D – Communicate with outside experts/vendors who receive GFE to support contract work with ATR.
Personal phone number	X	A, B, C & D	A/B - Database contains human resource data for all employees, including detailees, as downloaded from the National Finance Center. It is maintained by the HR staff and has limited controlled use. C/D – Communicate with outside experts/vendors who receive GFE to support contract work with ATR.
Medical records number			
Medical notes or other medical or health information	X	A	Database contains human resource data for all employees that is maintained by the HR staff and has very limited controlled use.
Financial account information	X	A	Database contains human resource data for all employees as downloaded from the National Finance Center, to include grade and step. It is maintained by the HR staff and has limited controlled use.
Applicant information			
Education records	X	A	Database contains human resource data for all employees as downloaded from the National Finance Center. It is maintained by the HR staff.
Military status or other information	X	A	Veteran's preference information used by HR staff in connection with hiring.

(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

Employment status, history, or similar information	X	A	Active status, dates of service, and similar information is maintained by HR staff.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A	Facilitate approval workflow for out-of-cycle GS step increases associated with sustained high-performance ratings.
Certificates	X	A	Process professional certifications for the purposes of intake and transfer to ATR's enterprise document management solution.
Legal documents			
Device identifiers, e.g., mobile devices	X	A	Mobile device identifiers (phone number and DOJ Tag#); Laptops, Servers, iPads, MS Surface Pros, RSA Tokens, monitors, docking stations, VTC equipment, printers, VOIP phones, etc. All ATR asset inventory is managed via ServiceNow®.
Web uniform resource locator(s)	X	A	ATR users access the ServiceNow® application via a link published on ATR's intranet page (ATRnet) that can be accessed through multiple approved web browsers.
Foreign activities	X	A	Workflow process of requesting the use of ATR assets during foreign travel is managed in ServiceNow®.
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			

(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

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**	X	A, B, C & D	
- **User passwords/codes**	X	A, B, C & D	Passwords are masked.
- **IP address**	X	A, B, C & D	
- **Date/time of access**	X	A, B, C & D	
- **Queries run**	X	A	Queries are run against the ServiceNow® database for auditing.
- **Contents of files**	X	A	Component employees responsible for administering and auditing the system have access to the contents of the files in the system.
Other (please list the type of info and describe as completely as possible):			

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

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax		Online	X
Phone	X	Email	X		
Other (specify): SNow's self-service portal allows users to update their personal information (such as personal email, home address, phone number). Users may have ability to reset network passwords using a one-time passcode to their cell phone or e-mail.					

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): Authorized users can download employee information from the National Finance Center for government staff and detailees. Authorized users can upload employee records to eOPF; employees can also download their personal records from eOPF.					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	X
Commercial data brokers					
Other (specify): Contact information stored for outside experts and vendors who receive GFE to support contract work with ATR.					

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.

	How information will be shared			
Recipient	**Case-by-case**	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X	X	X	Authorized ATR users can share information within ATR on a case-by-case basis either from the system and in accordance with organizational rules, for instance to facilitate HR functions. Most of the information sharing is performed using direct log-in. Bulk transfers can be performed within the Component, as needed.
DOJ Components	X			Authorized ATR users can share or receive information with or from other DOJ Components on a case-by-case basis either from the system and in accordance with organizational rules, for example detailee information.
Federal entities		X	X	Authorized ATR users can download information from other Federal entities, for instance from USA Hire and Staffing, USA Performance, and the National Finance Center to facilitate HR functions, and upload or download data to eOPF, on a regular basis from the system and in accordance with organizational rules.
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.

Information from SNow will not be released to the public for Open Data purposes.

Section 5: Notice, Consent, Access, and Amendment

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

DOJ provides the public with generalized notice about its collection, use, and sharing of PII through a variety of Systems of Records Notices (SORNs), and, in some instances, individualized notice pursuant to Section 552a(e)(3) of the Privacy Act. In this case, one (1) ATR SORN and three (3) DOJ SORNs, described in section 7.2 of this document, provide generalized notice to the public.

Some information from ATR Application Management Suite (ATR AMS) has been migrated to SNow, specifically HR data and surveys. This information was covered in the PIA for ATR AMS (https://www.justice.gov/d9/2023-04/atr_ams_pia.pdf).

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals generally do not have the opportunity to decline the use or dissemination of their information collected in ATR SNow. Information in ATR SNow is generally collected from other systems, such as National Finance Center (NFC) data, USA Hire and Staffing, and USA Performance. Employee data uploaded to eOPF are official employee records.

In addition, ATR SNow collects information from visitors to the system, such as user IP addresses, the date and time of access, queries run, and the content of files accessed and reviewed. ATR users can update their contact information that is displayed on the ATR internal network ("intranet") page using the ServiceNow® self-serve portal but cannot opt out of audit logs for their use of the 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.

All such requests may be submitted to the ATR FOIA/Privacy Act Unit (https://www.justice.gov/atr/antitrust-foia) for processing and response.

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):** September 23, 2024 **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 (POA&Ms) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POA&M documentation:** No identified risks.
	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	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** ATR SNow is categorized as a moderate system based on a review of the aggregate impact levels for confidentiality, integrity, and availability.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The system has not undergone a full security assessment in accordance with the DOJ Security and Privacy Assessment and Authorization Handbook, but the system categorization has been completed, as indicated below. ATR recently received an award to purchase, migrate data, and customize a version of ServiceNow® for ATR's requirements. The highest sensitivity information contained on this system pursuant to the Federal Information Processing Standards (FIPS) security categorization(s), as defined in NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, is Moderate and matches the most sensitive information in the system, per the 'high water mark' standard. The ServiceNow® GCC is hosted within its own datacenters. System documentation supporting ATR SNow activities are maintained within the Department's system of record, Joint Cybersecurity Authorization Management (JCAM), tool. ATR acknowledges that any suspected or confirmed incident or breach to the system will be reported to the Contracting Officer Representative and Justice Security Operations Center (JSOC).

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:** ATR SNow satisfies the Audit and Accountability (AU) controls outlined by NIST 800-53, Rev.5, Security and Privacy Controls for Information Systems and Organizations. All approved policies, procedures, standards, and program plans fully meet the requirements of FISMA.
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**: Welcome to ServiceNow® training is available for all of ATR's users (how to use the interface for ATR SNow). Advanced training courses are required for HR and IT staffs.

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?

ATR personnel, both government and contractor, sign the DOJ Rules of Behavior prior to being granted access to the ATR network, and annually thereafter as a part of the DOJ cybersecurity awareness training. ATR users are required to use multi-factor authentication, or unique usernames and passwords, to access the ATR network. ATR SNow depends on active directory services to support a single sign-on solution and to audit unauthorized access to the ATR network and its applications. Audit logs are maintained and managed using Splunk.

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.)

Requirements governing retention and disposition of ATR documents and information are documented within ATR Directive 2710.1: "Procedures for Handling Division Documents and Information," consistent with National Archives and Records Administration regulations and rules.

<u>Section 7</u>: 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:

- ATR-005, "Antitrust Management Information System (AMIS) - Time Reporter," 53 Fed. Reg. 40502 (10-17-1988), 66 Fed. Reg. 8425 (1-31-2001), 82 Fed. Reg. 24147 (5-25-2017)
- DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 64 FR 73585 (12-30-1999), 66 FR 8425 (1-31-2001), 82 FR 24147 (5-25-2017), 86 FR 37188 (7-14-2021). Exemptions Claimed Pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). *See* 86 FR 61687
- DOJ-009, "Emergency Contact Systems for the Department of Justice," 69 Fed. Reg. 1762 (1-12-2004), 82 Fed. Reg. 24147 (5-25-2017)
- DOJ-014, "Department of Justice Employee Directory Systems," 74 Fed. Reg. 57194 (11-4-2009), 82 Fed. Rg. 24151, 153 (5-25-2017)

<u>Section 8</u>: 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.***

To mitigate the risk of collecting inaccurate or outdated information, ATR has implemented series of checks and balances to ensure that only applicable and accurate information is stored in the system.

The sources of information for ATR SNow are as follows:

1. Human resource data for all employees as downloaded from the National Finance Center, which is maintained by the HR staff and has limited controlled use;
2. Data for potential government appointees, which shared bi-directionally from USA Hire and Staffing as a subscriber to the application;
3. Data for government personnel performance reviews, which is ingested from USA Performance;
4. Official government employee records, which are uploaded to eOPF; and
5. Data input directly by ATR users into the ATR SNow application, as needed.

ATR follows a records retention schedule, and policies designed to prevent the maintenance of data that is no longer needed to fulfill the mission. Requirements governing the retention and disposition of ATR documents and information are documented within ATR Directive 2710.1: Procedures for Handling Division Documents and Information, consistent with National Archives and Records Administration regulations and rules.

To mitigate the risk of unauthorized access into the system, ATR establishes control over information contained in ATR SNow by strictly managing and monitoring access control, based on user roles and permissions, to include HR-related information. DOJ background checks are performed on all DOJ personnel, including ATR employees and contractors. In addition to background checks, all ATR personnel are required to complete annual computer security awareness training and sign the DOJ Cybersecurity and Privacy Rules of Behavior (ROB) for General Users (GROB) which include rules for safeguarding identifiable information, and annually thereafter as a part of the DOJ cybersecurity awareness training. Detailed privacy training is also required for all ATR users.

Additionally, ATR personnel requiring privileged access to ATR SNow are required to sign the DOJ Cybersecurity and Privacy ROB for Privileged Users (PROB).

ATR users are required to use multi-factor authentication, or unique usernames and passwords, to access the ATR network. ATR SNow depends on active directory services to support a single sign-on solution and to audit unauthorized access to the ATR network and its applications. Audit logs are maintained and managed using Splunk.