Federal Trade Commission
Privacy Impact Assessment

ServiceNow
General Service Platform

Updated February 2025

Table of Contents

1 System Overview 1

2 Data Type, Sources, and Use 2

3 Data Access and Sharing 7

4 Notice and Consent 8

5 Data Accuracy and Security 10

6 Data Retention and Disposal 11

7 Website Privacy Evaluation 12

8 Privacy Risks and Evaluation 12

1 System Overview

1.1 Describe the project/system and its purpose.

The FTC has contracted with Leidos to use a Software-as-a-Service (Saas) model for its Enterprise Service Management (ESM) known as the ServiceNow Service Automation Government Cloud Suite (ServiceNow). ServiceNow is comprised of a suite of integrated applications designed to support IT service automation, resource management, and shared support services at the FTC. Listed below are examples of ServiceNow applications that are currently in use at the FTC: [1]

- **IT Service Management (ITSM)** – the system is generally utilized to provide ITSM functions for the FTC, to include maintenance of a database of IT users, IT assets, non-IT assets, configurations, incidens, and requests. The ITSM platform allows for submission and tracking of IT and business requests, incidents, forms, and data. Additionally, the Office of the Chief Information Officer (OCIO) and the Office of the Chief Privacy Officer (OCPO) use the ServiceNow platform to support the incident reporting and hardware asset management processes.
- **HR Service Delivery (HRSD)** – the FTC's Human Capital Management Office (HCMO) uses the HRSD application to streamline and automate the agency's human resources processes including new hire onboarding, security investigations, and access requests;
- **Nuvolo Facilities Enterprise Asset Management (EAM)**: this application is used by the Office of the Chief Administrative Services Officer (OCASO) to streamline and automate space and facilities management at the FTC, including facilities maintenance, asset management, and space management.
- **Division of Litigation Technology & Analysis (DLTA) application** – the DLTA application serves as a portal for request submission, management, tracking, and reporting of requests related to FTC investigations.
- **Administrative E-Filing** – the E-Filing system is set up to facilitate submission, tracking, and management of public and nonpublic filings via electronic means, including electronic service of public filings, and web postings of such filings in the FTC's adjudicative proceedings conducted under Part 3 of the Commission's Rules of Practice, 16 C.F.R. pt. 3.
- **Print Tracking** – the Print Tracking application provides the tracking of print publication inventory, budget, and order information so that the FTC can maintain inventory, minimize costs, and report on outreach efforts.

[1] This PIA addresses the FTC's general use of the ServiceNow framework to collect, process, disseminate, and store information in the ServiceNow cloud in support of the Agency's mission. Additional system specific PIAs (e.g., Administrative E-Filing, Print Tracking) that are hosted on the ServiceNow platform are available on www.ftc.gov.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The information in this system is collected, maintained and disseminated pursuant to the agency's authority to administer its operations and programs under the Federal Trade Commission Act, 15 U.S.C. §§ 41-58 and other laws and regulations the Commission enforces. System user information is also collected and maintained for system security and administration purposes under the Federal Information Security Modernization Act of 2014 and other applicable Federal information security laws, regulations, orders, guidance, and policies.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[2] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.

☒ Full Name
☒ Date of Birth
☒ Home Address
☒ Phone Number(s)
☒ Place of Birth
☒ Age
☒ Race/ethnicity
☒ Alias
☒ Sex
☒ Email Address
☒ Work Address
☒ Taxpayer ID
☒ Credit Card Number
☒ Facsimile Number
☒ Medical Information
☒ Education Records
☒ Social Security Number
☒ Mother's Maiden Name

☒ Biometric Identifiers (e.g., fingerprint, voiceprint)
☒ Audio Recordings
☒ Photographic Identifiers (e.g., image, x-ray, video)
☒ Certificates (e.g., birth, death, marriage, etc.)
☒ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)
☒ Vehicle Identifiers (e.g., license plates)
☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)
☒ Geolocation Information
☒ Passport Number

☒ User ID
☒ Internet Cookie Containing PII
☒ Employment Status, History, or Information
☒ Employee Identification Number (EIN)
☒ Salary
☒ Military Status/Records/ ID Number
☒ IP/MAC Address
☒ Investigation Report or Database
☒ Driver's License/State ID Number (or foreign country equivalent)
□ Other *(Please Specify)*:__

Note: While ServiceNow may not directly collect this information from members of the public, the FTC might obtain this data as part of its law enforcement and other activities and maintain it within the ServiceNow platform. This may include all types of PII and sensitive information and is not limited to the data elements identified in the above table.

[2] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

Non-PII collected or maintained by the system includes data collected by the system's IT Service Management functions. This data includes not only PII (e.g., names of individuals associated with service requests), but also non-PII such as IT assets, non-IT assets, configurations, incidents, and requests.

Documents uploaded to the ServiceNow platform may include law enforcement related documents and other types of documents. Examples of law enforcement related documents in the system include compulsory process documents (e.g., subpoenas and civil investigatory demands); investigative hearing transcripts, transcripts of depositions in adjudicative proceedings, transcripts of adjudicative hearings and trials; briefs and other documents filed in adjudicative proceedings; orders entered in adjudicative proceedings; briefs and other documents filed in federal court cases; federal court orders to pay consumer redress and financial statements from individuals ordered to pay redress; Federal Register Notices of proposed consents; petitions related to cease and desist orders and FTC responses.

2.3 What is the purpose for collection of the information listed above?

Information is mainly collected and utilized within the ServiceNow platform for the purposes of providing an Information Technology Service Management (ITSM) platform, allowing for submission and tracking of IT and business requests, incidents, forms, and data. FTC users can access the ServiceNow application through the Internet via their FTC laptop or via the NowMobile application. The Now Mobile app is a downloadable app that FTC users can use to submit requests and issues, find answers using global search and knowledge base, and/or view and report issues around the user's assets.

The ServiceNow portal allows staff and contractors to request new hardware or software, report incidents involving lost or misplaced data, or place other IT related inquiries. IT related tickets concerning hardware, software, and misplaced/lost equipment are received by FTC Help Desk staff, who use the information provided by staff to address, approve, and close tickets. Privacy incidents involving loss or suspected loss of personally identifiable information (PII) or nonpublic information are addressed by OCPO and, as needed, the Office of General Counsel (OGC). OCPO also use the information provided by staff to conduct incident investigations, assess risk, and take mitigating steps to close out an incident. Only limited authorized users have access to all data in the incident response portal. Individual FTC users can only see the tickets that he/she has submitted.

HCMO and OCASO use the ServiceNow HRSD and Nuvolo applications to coordinate and streamline the agency's new hire onboarding process. Once an individual has been cleared for hire and HCMO has established a start date, the hiring manager receives an automatic notification to submit a Nuvolo space assignment request through ServiceNow. Upon entry of the new hire's name, the request automatically populates with the new hire's details, allowing the hiring manager to request a space assignment using Nuvolo's floor map features. When the new employee has a space assigned, all notifications and work order tasks are sent automatically to staff in Facilities, Customer Service, Physical Security, and Information Technology Management offices, so that they can begin their activities in support of onboarding the new employee. HCMO staff can then track the status of these tasks through a dashboard; Administrative Officers, Supervisors, Hiring Managers, and Contracting Officer Representatives can also track the status of their new employees as they onboard.

The Bureau of Consumer Protection's Division of Litigation Technology & Analysis (DLTA) uses ServiceNow for request submission, management, tracking, and reporting of requests related to FTC investigations. This information may contain personally identifiable information (PII) as well as other types of sensitive data. Specifically, for each agency matter, the system database contains the names, addresses, and certain other information on persons and organizations within and outside the FTC associated with that matter (e.g., FTC attorneys, economists, or other staff assigned to work on the matter, as well as defendants, opposing counsel, intervening parties, etc., who may be involved in the matter).

For more information on the purpose of collection relevant to the Administrative E-Filing application as well as the Print Tracking application, please refer to the specific PIAs for those applications available on www.ftc.gov.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	*Type of Data Provided & How It Is Collected*
FTC Employees and Contractors	**HRSD** – FTC HCMO staff use the HRSD application to streamline and automate the aency's human resources processes including new hire onboarding, security background investigations, and physical or logical and access requests. Upon entry of the new hire's name, the request automatically populates with the new hire's details, allowing the hiring manager to request a space assignment using Nuvolo's floor map features.
	Nuvolo – Personnel provide data for the purpose of building and facilities maintenance, asset management, and space management. Scenarios requiring input from staff include but are not limited to: • Facility Work Order Creation • Improvement requests • Furniture moves • Personnel On/Off-boarding Process • Personnel Moves/Changes

Source of Data	*Type of Data Provided & How It Is Collected*
	IT Service Management (ITSM) – Generally utilized to provide ITSM functions for the FTC, which includes maintenance of a database of IT users, IT assets, non-IT assets, configurations, incidens, and requests. The ITSM platform allows for submission and tracking of IT and business requests, incidents, forms, and data. Additionally, the Office of the Chief Information Officer (OCIO) and the Office of the Chief Privacy Officer (OCPO) use the ServiceNow platform to support the incident reporting and hardware asset management processes, detailed below.**ServiceNow Incident Response Portal** – When an FTC employee/contractor wishes to submit an IT-related request, they must sign into the ServiceNow portal using their FTC-issued computer and/or mobile device. Due to the platform's integration with Okta Single Sign-On, the employees location, room number, organization are automatically populated in the request form. The requester can describe the item or service needed in an open text field. If reporting a lost or misplaced item of equipment (e.g., PIV card, FTC mobile phone, FTC laptop, FTC thumb drive, etc.), the requester must also submit a Lost Equipment Reporting ticket. The form contains information about the reporting individual (name, organization code, phone number, name of supervisor), and also requires additional descriptions of how and where the loss occurred. Similarly, when reporting a privacy incident, the employee/contractor office location, room number, and organization code are automatically populated in the ServiceNow portal. Additionally, the requester is required to indicate the date and time of the incident, as well as a description of what and how the incident occurred, and whether the incident has been reported to law enforcement. Optional data fields allow the requester to select PII elements involved in the incident and provide more information about the incident such as mitigating steps and number of individuals affected; they can also upload/attach any supporting documentation. The supporting documentation could contain any and all kinds of data, depending on the incident.

Source of Data	***Type of Data Provided & How It Is Collected***
	DLTA Application – This portal is used for submission, management, tracking, and reporting of requests related to FTC investigations. DLTA staff receive evidence in many different forms (paper, hard drives, CD/DVDs, thumb drives, etc.) from parties both internal and external to the FTC. The DLTA application effectively tracks the evidence from initial receipt to final disposition using a detailed inventory of the item (serial number and/or description, location stored, and matter name/number) and ensuring proper chain of custody.
Members of the Public	**ServiceNow Administrative E-Filing**[3] – Admin E-Filing allows users to submit public and nonpublic pleadings and motions in Part 3 administrative litigations before the Administrative Law Judge (ALJ) and the Commission. In order to use the application, a user (i.e., lawyers or paralegals representing respondents or third parties in the Part 3 matter) must register with a unique user ID and password. The user's name, company name, work address, work telephone number, work email address, and bar admission number (if applicable) are required to register. **ServiceNow Print Tracking**[4] – The FTC uses the ServiceNow Print Tracking application to track the types and number of publications printed from online print orders received through bulkorder.ftc.gov. This information can include the customer's full name, email address, work address, and phone number(s). The FTC user's login information (user ID, time of login and logout), as well as roles and access permission levels, are maintained within the ServiceNow system.
FTC General Support System (GSS)	The GSS serves as the primary IT infrastructure used by the FTC to host information systems that collect, process, disseminate, and store information in support of the Agency's mission. The GSS hosts most of the FTC's systems, subsystems, databases, and applications. Integration of the GSS with ServiceNow is a necessity to facilitate the Enterprise Service Management capabilities such as service automation, resource management, and shared support services at the FTC.
FTC Matter Management System (MMS)	MMS is integrated with ServiceNow in support of the DLTA service in order to facilitate the population of information related to existing FTC matters and investigations.

[3] For more information, refer to the ServiceNow Administrative E-Filing PIA on www.ftc.gov.

[4] For more information, refer to the ServiceNow Print Tracking Application PIA on www.ftc.gov.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC staff and contractors	ServiceNow is only accessible to authorized users using an FTC-issued computer or mobile device on the FTC network or through a secure FTC connection. Help Desk and OCIO staff use the data provided in the service portal to address IT related requests and equipment loss incidents. OCPO staff utilize data in the ServiceNow incident response portal to catalog and track privacy incidents. HCMO staff are able to view and catalog sensitive personnel information in order to perform security case management. OCASO staff use the Nuvolo application to perform facilities management functions within ServiceNow. Authorized ServiceNow administrators have access to system data for troubleshooting and maintenance purposes. BCP's DLTA staff have access to information submitted through the DLTA portal for purposes related to FTC investigations.
ServiceNow Cloud Service Provider	The ServiceNow Cloud Service Provider does not have access to FTC data because the data stored in ServiceNow is encrypted, and the data can only be accessed from the FTC network with authorized FTC user accounts.
Members of the Public	In order to use the ServiceNow Administrative E-Filing application, a user (i.e., lawyers representing respondents or third parties in the Part 3 matter) must register with a unique user ID and password. The user's name, company name, work address, work telephone number, work email address, and bar admission number (if applicable) are required to register. Users can log into their account and access limited personal information about themselves, such as their password and security questions. They do not have the ability to change their profile information or access log details about their activities.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Yes, authorized FTC contractors have access to information in the various systems and programs that are currently included on the ServiceNow platform. Some authorized FTC contractors have access to ServiceNow simply as users, and one or more authorized FTC contractors has access to certain administrative functions.

All FTC contractors are required to sign NDAs, complete security and privacy training prior to obtaining access to any FTC systems, and complete annual security and privacy training to maintain network access and access to those systems.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

FTC contractors and authorized ServiceNow system administrators who have access to the ServiceNow platform are subject to the same agency rules and policies followed by FTC staff. All contractors must also abide by the FTC's Breach Notification Response Plan in the event of an incident or breach.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

□ Notice is provided via (*check all that apply*):

□ Privacy Act Statement (□ Written □ Oral)
□ FTC Website Privacy Policy
□ Privacy Notice (e.g., on Social Media platforms)
□ Login banner
□ Other

(*explain*):____

☒ Notice is not provided (explain): The ServiceNow platform is comprised of various applications that collect and maintain PII. Neither those applications or nor ServiceNow are the original collection points of PII, where notice would be provided. Instead, Privacy Act statements are included on forms, websites, and other instruments by which Privacy Act information is collected from members of the public, either in written or oral form. For those occasions where the FTC cannot provide notice at the time the information is collected, the FTC provides notice via its privacy policy, its Privacy Act system of records notices (SORNs), and its PIAs, including this one. Users of ServiceNow are presented with login banners when logging into the FTC's network, before accessing ServiceNow.

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

In some cases, it is not possible for users to decline to provide information or to consent to the use of their information. Those who provide information pursuant to compulsory process do not generally have a right to decline to provide the information. Likewise, new hires must provide their information for HCMO and OCASO to use in the HRSD and Nuvolo applications to coordinate and streamline the agency's new hire onboarding process. In other cases, submitting PII is voluntary as a legal matter, but failure to submit the PII will mean denial of system access or service. For example, staff and contractors reporting privacy incidents or IT related issues must provide information about themselves so that the FTC Help Desk and OCPO can address their requests.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

FTC employees and contractors who use the ServiceNow incident reporting portal have access to information about themselves when they submit a request or report an incident (i.e., the requester can review the request or report and receive confirmation of the information they have submitted to the system).

In cases where the subject individual does not have such system access, the individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in the Privacy Act systems that are hosted on the ServiceNow platform. The FTC's privacy policy provides links to the FTC's SORNs, as well as information about making Freedom of Information Act (FOIA) requests and the online FOIA request form. Individuals must follow the FTC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) at 16 C.F.R. 4.13. Access to information under the Privacy Act is subject to certain exemptions.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

The FTC provides a process for individuals to correct or amend any inaccurate PII maintained by the FTC, including any information that may be stored in the ServiceNow platform. The FTC's Privacy Policy provides links to the FTC's SORNs, which include information about how to correct or amend records that are subject to the Privacy Act, under the same procedures for accessing such records. See section 4.3. Where appropriate, the FTC disseminates corrected or amended PII to other authorized users of that PII. Furthermore, in some cases, as noted in section 4.3, subject individuals can access the system and correct their own information (e.g., update or cancel their IT service request).

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

Due to the nature of the system and the anticipated broad use of these services across the enterprise, information that is stored in ServiceNow generally will not be checked for accuracy, completeness, or currency. It is the responsibility of the user to ensure the completeness, accuracy, and currency of data at the time it is created or used (e.g., individuals requesting IT services may supplement, update, or cancel their service request in the system).

However, information maintained in Service Now that is used by the FTC as part of its law enforcement and other activities will be reviewed for accuracy and timeliness as required by the particular activity and the laws and authorities, if any, applicable at the time the agency compiles the records (e.g., FTC Act, personnel laws, administrative or court evidentiary rules and procedures).

System administrators ensure user information is complete and accurate for access control through enterprise directory authentication, but will not ensure that data created or entered by end users is complete, accurate, or current. The User Directory is updated immediately when a user account is disabled or terminated. User contact information is removed once the user account is deleted. Within the organization, users have the ability to enter their own information and to ensure that it is current.

All information in the FTC GSS, including the information stored in ServiceNow Cloud, is also subject to appropriate information security controls, as further described below in this PIA and the GSS PIA. These controls will ensure that sensitive information is protected from any undue risk of loss and that the contents of evidentiary materials remain unchanged from the time they are included in the GSS. The GSS facilitates the data gathering functionality and once data is collected, it is uploaded to the ServiceNow Cloud for processing and storage.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

There are administrative procedures, technical safeguards, and controls in place to protect and ensure proper use of data in ServiceNow. All authorized users are required to use two-factor authentication to access the application. FTC users of the application must use their PIV cards along with a PIN to access data in the system. External users must authenticate with a registered username and password and agree to receive a one-time passcode (OTP) by voice or use an OTP token authenticator app on their smartphone in order to use the application. Additional safeguards for FTC users include role-based access controls at the application level to control who has access to what data in the application.

The principle of least privilege is used to grant access, and user actions are tracked in the ServiceNow audit logs. Other procedures, technical safeguards, and controls that protect data in ServiceNow pertain to the FedRAMP authorization that ServiceNow was granted. All FTC positions are assigned a risk designation that has associated criteria for personnel screening. All potential FTC staff, contractors, and volunteers are subject to background investigations and suitability reviews in accordance with OPM guidance. Before any new employee, contractor, or volunteer can access any application within ServiceNow, that individual must first attend new employee orientation and successfully complete the FTC's Information Security Awareness and Privacy training. All staff are granted basic network access to include email services, the Internet, the Intranet, network shared drives, network-based applications, and are assigned their own home directory. Categories of staff with temporary agency affiliation – such as interns and International Fellows – may have restricted network and physical access.

Supervisors and/or Contracting Officer's Representatives (CORs) must identify and approve employee requests to access network applications and specify the appropriate user role and level of access privileges. Auditing measures and technical safeguards are in place commensurate with the Moderate-Impact Baseline of the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations Special Publication (SP) 800-53 Revision 5.

FTC staff is responsible for minimizing PII and disposing of it when the PII is no longer needed and in accordance with the FTC records disposition schedule. The FTC ensures that all staff and contractors annually electronically certify their acceptance of FTC privacy responsibilities and procedures by requiring comprehensive Information Security Awareness and Privacy training. Moreover, all staff must annually acknowledge procedures for handling PII – including minimizing PII – and attest that all PII maintained by the individual has been properly secured and accounted for as part of the FTC's annual privacy and security training.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

☒ Not Applicable

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

In accordance with the National Archives and Records Administration (NARA) guidelines, General Records Schedule 3.2, records will be purged following the third fiscal year of retention, under disposition authority DAA-GRS-2013-0006-0002. Records will be flagged at their date of closure and purged based on that date. Records will simply be deleted in a batch from the ServiceNow system, and will no longer be accessible to any system user.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

The ServiceNow environment is a web-based application. ServiceNow utilizes both session-based and persistent-based cookies to enable core site functionality.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	***Mitigation Strategy***
Misuse of data by authorized users	Prior to receiving access to the FTC's network, all users must agree to the FTC Rules of Behavior, which includes consent to monitoring and restrictions on data usage.
Unauthorized system access	All FTC users must have a government-issued personal identity verification (PIV) card to access ServiceNow. FTC's user identity management processes include authentication with enterprise directory to control and manage access restrictions to authorized personnel on an official need-to-know basis. The FTC utilizes a combination of technical and operational controls to reduce risk in the ServiceNow environment, such as encryption, passwords, audit logs, firewalls, malware identification, and data loss prevention policies. As a FedRAMP-approved cloud service provider, ServiceNow undergoes regular reviews of its security controls. External users must authenticate their ServiceNow account with a registered username, password, and one-time passcode (OTP) by voice or use an OTP token authenticator app on their smartphone in order to use the application.
Data leakage	The contract between FTC and ServiceNow does not allow the service provider to review, audit, transmit, or independently store FTC data, which minimizes privacy risks from the vendor source.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

User access is managed through the FTC's enterprise directory infrastructure, which uniquely identifies, authenticates, and applies permissions to authorized user sessions based on FTC policies and procedures. This allows the FTC to leverage organizational multifactor authentication solutions, including HSPD-12, already deployed to meet internal identification and authentication requirements. The use of enterprise directory service also allows automatic enforcement of certain policies and requirements, such as password complexity and maximum-log in attempts, for organizational users. Additionally, FTC security policies require automated monitoring of information system components with regard to flaw remediation.

The ServiceNow E-Filing application includes an automatic logoff after 15 minutes of inactivity, deactivating users after 35 days of account inactivity, and locking user accounts after 3 incorrect password attempts.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

SORNs that cover relevant information collected by other systems, to the extent such information is maintained and retrieved by name or other personal identifier in ServiceNow, are accessible at www.ftc.gov. This includes, for example: system user information, see VII-3 -- Computer Systems User Identification and Access Records – FTC; records of IT service requests, see VII-7 -- Information Technology Service Ticket System – FTC; investigatory or other program records, see I-1 -- Nonpublic Investigational and Other Nonpublic Legal Program Records – FTC; records relating to personnel security and background investigations, see II-11 -- Personnel Security, Identity Management, and Access Control Records System – FTC; records of accountable property assigned to employees and contractors, see VII-5 -- Property Management System – FTC; etc.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The administrative and technical controls described in section 5.2 of this document provide assurance that the collection, use, and maintenance of the information will be conducted as described in this PIA. This PIA aligns with the FTC's existing privacy policies and procedures.