



UNITED STATES  
**FEDERAL COMMUNICATIONS COMMISSION**  
INFORMATION TECHNOLOGY


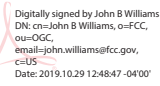
# **PRIVACY IMPACT ASSESSMENT FOR THE SERVICENOW SYSTEM**

10/29/2019

**OFFICE OF THE MANAGING DIRECTOR**

445 12TH STREET SW, WASHINGTON, DC 20554

## Record of Approval

Document Approval		
<Document POC>		
Printed Name: Bahareh Moradi		
Signature: 	Date 10/25/19	
<Approval Structure>		
Printed Name: John Williams		
Signature: John B Williams 	Date 10/29/19	
Printed Name:		
Signature:	Date	

## Record of Approval

Date	Description	Author

# Table of Contents

---

<b>ServiceNow.....</b>	<b>4</b>
1.1. INTRODUCTION .....	4
1.2. SYSTEM OVERVIEW.....	5
1.3. NATURE AND USE OF THE INFORMATION THAT WILL BE COLLECTED .....	7
1.4. DATA SECURITY .....	11
1.5. ACCESS AND SHARING OF THE INFORMATION .....	11
1.6. PRIVACY ACT SYSTEM OF RECORDS NOTICE .....	12

# List of Tables

---

Table 1-1: PII Elements Table.....	7
Table A-1: Acronyms and Abbreviations.....	A-1

## [System Name]

### 1.1. Introduction

Section 208 of the E-Government Act of 2002<sup>1</sup> requires agencies to conduct a **Privacy Impact Assessment (PIA)** whenever they procure or develop an information technology system that will collect, maintain, or disseminate information about individual people. The PIA must document how the system will use information it collects about individuals and, unless it contains classified or sensitive information, it must be made available to the public. The PIA was intended to be a tool for agencies to protect personal information throughout a technology system's life cycle. The Office of Management and Budget (OMB) has commented: *"In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks."*<sup>2</sup>

The FCC is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below explore important privacy issues identified in the Act and in later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). A longer discussion of the FCC's PIA policies can be found in Chapter 9 of the FCC's Privacy Act Manual (FCC Inst. 1113.1).

In accordance with FCC policy, system owners should complete the **Initial Privacy Assessment (IPA)** prior to filling out the PIA. The IPA helps system owners determine whether their systems will collect the kind of information that would make them subject to the requirements of Section 208. The PIA should not be completed if the IPA has not yet been completed first since it determines if your system requires a PIA.

If you have any questions, please contact the Privacy Manager, Les Smith, at [leslie.smith@fcc.gov](mailto:leslie.smith@fcc.gov) or 202-418-0217.

---

<sup>1</sup> 44 U.S.C. § 3501 note.

<sup>2</sup> OMB Memorandum No. M-03-22 (Sep. 26, 2003), [https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03\\_22.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf).

## 1.2. System Overview

**A. Avoiding technical terms and unexplained abbreviations, please provide a general description of this information system.**

ServiceNow provides application suites and software solutions as well as a single, mobile, and web application development platform to build, customize, and automate applications and workflow at the FCC.

The FCC uses ServiceNow to build and operate a number of different applications that help the FCC conduct its business. Applications currently operating on ServiceNow include systems that process FCC employee information, that track and manage internal FCC processes, and that provide a means for outside organizations to report information to the FCC. Because the FCC continues to develop applications using ServiceNow, this PIA covers both the FCC applications that currently operate on this platform and similar applications it will develop in the future.

**B. Is this a new information system or a significant revision of an existing system?**

New System

Revision of Existing System: Please describe the revision that will be made to an existing system.

**C. Why is the FCC developing, procuring, or revising this information system? What is the purpose of this system?**

ServiceNow allows the FCC to streamline and simplify application development and support by providing an existing infrastructure that can be modified and customized depending on Bureau or Office needs.

**D. If this system is going to be provided through a cloud-based computing system,<sup>3</sup> please check the box that best describes the service the FCC receives from the cloud computing provider:**

---

<sup>3</sup> See NIST, *The NIST Definition of Cloud Computing*, Special Pub. No. 800-145 (Sep. 2011), <https://csrc.nist.gov/publications/detail/sp/800-145/final>.

- The FCC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS)
- The FCC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service or PaaS)
- The FCC has deployed its own application/s on the cloud network and controls how these application/s are configured and operate (Infrastructure as a Service or IaaS)

**E. Under what legal authority is the FCC developing, procuring, or revising this information system?**

The information in this system is collected, maintained, and disseminated pursuant to the Communications Act of 1934, as amended, and [other rules and regulations](#) the FCC enforces.

### 1.3. Nature and Use of the Information that will be Collected

A. Specify in the table below what types of personally identifiable information (PII) may be collected, maintained, or processed in this information system.<sup>4</sup> Check all that apply and add any types that are not listed below.

Table 0-1: PII Elements Table

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
<input checked="" type="checkbox"/> Full Name <input checked="" type="checkbox"/> Date of Birth <input checked="" type="checkbox"/> Home Address <input checked="" type="checkbox"/> Phone Number(s) <input checked="" type="checkbox"/> Place of Birth <input checked="" type="checkbox"/> Age <input checked="" type="checkbox"/> Race/ethnicity <input type="checkbox"/> Alias <input checked="" type="checkbox"/> Sex <input checked="" type="checkbox"/> Email Address <input checked="" type="checkbox"/> Work Address <input checked="" type="checkbox"/> Taxpayer ID <input type="checkbox"/> Credit Card Number <input type="checkbox"/> Facsimile Number <input checked="" type="checkbox"/> Medical Information <input checked="" type="checkbox"/> Education Records <input checked="" type="checkbox"/> Social Security Number <input type="checkbox"/> Mother's Maiden Name	<input type="checkbox"/> Biometric Identifiers (e.g. fingerprint, voiceprint) <input type="checkbox"/> Audio Recordings <input type="checkbox"/> Photographic Identifiers (e.g. image, x-ray, video) <input type="checkbox"/> Certificates (e.g. birth, death, marriage, etc.) <input type="checkbox"/> Legal Documents, Records, Notes (e.g. divorce decree, criminal records, etc.) <input type="checkbox"/> Vehicle Identifiers (e.g. license plates) <input type="checkbox"/> Financial Information (e.g., account number, PINs, passwords, credit report, etc.) <input type="checkbox"/> Geolocation Information <input type="checkbox"/> Passport Number	<input type="checkbox"/> User ID <input type="checkbox"/> Internet Cookie Containing PII <input checked="" type="checkbox"/> Employment Status, History or Information <input type="checkbox"/> Employee Identification Number (EIN) <input checked="" type="checkbox"/> Salary <input type="checkbox"/> Military Status/Records/ID Number <input type="checkbox"/> IP/MAC address <input type="checkbox"/> Driver's License/State ID Number (or foreign country equivalent) <input checked="" type="checkbox"/> Other (Please Specify):

**Other:** Most of the FCC applications that currently operate on the ServiceNow platform do not collect or maintain personally identifiable information (PII) directly from members of the public.

The Auctions and Universal Licensing System (AULS), built on the ServiceNow Platform collects phone numbers, email addresses, and occasionally tax ID numbers from individual members of the public.

<sup>4</sup> The Office of Management and Budget (OMB) defines PII as, "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." OMB Circular No. A-130, "Managing Information as a Strategic Resource" (2016), 33.

Some FCC applications that currently operate on the ServiceNow platform pertain to the internal operations of the FCC and maintain PII from members of the public applying for jobs at the FCC. The FCC’s EEO Complaint system maintains PII including name, date of birth, home address, phone number, place of birth, age, race/ethnicity, sex, email address, work address, medical information, education records, social security numbers, employment status/history or information, and salary for employees or job applicants who have filed EEO complaints against the FCC.

Other FCC applications related to the internal operations of the agency collect and maintain employee PII including name, date of birth, home address, phone number, place of birth, age, sex, email address, work address, social security numbers, employment status/history or information, and salary.

To the extent PII is stored in other FCC applications on ServiceNow, the information collection is incidental.

**B. Please explain why it is necessary to collect these PII data elements to carry out the purpose of this system.**

Information in ServiceNow applications is collected, used, disseminated, and maintained for the FCC to perform a variety of regulatory, licensing, enforcement, policy, personnel management, and other activities. PII may be present in some of these activities.

**C. Will this PII be collected from individuals themselves, or from third parties?**

Source of Data	Type of Data Provided and How it is Collected
FCC Staff and Contractors	FCC staff and contractors upload data that has been created or obtained in connection with the Commission’s regulatory, licensing, enforcement, personnel and security management, and other activities. Several FCC administrative and human resources applications that operate on this platform collect and maintain PII provided by FCC employees and contractors.
Members of the Public	A small amount of information provided by and pertaining to members of the public is stored in FCC applications on ServiceNow. For the majority of the FCC’s applications on ServiceNow, the information is incidentally collected and stored.

**D. Will individuals be able to consent to the collection or particular uses of the information? What will the form of the consent be? What happens if individuals do not consent to the collection or particular uses?**



The opportunity or right depends on how the information is collected. The FCC generally does not use ServiceNow to collect information, including PII, directly from the public. However, FCC staff and contractors use ServiceNow for operational, personnel, and security management, or in furtherance of the FCC's enforcement or policy mission. To the extent information collected through applications built on the ServiceNow platform or from other sources incidentally includes PII, individuals will not have an opportunity to consent.

Members of the public use AULS, an FCC application built on the ServiceNow platform, to submit filing questions or report technical issues to the FCC. In these instances, the FCC collects information necessary for resolution and response of these requests. An individual requesting resolution or response through AULS has implied consent.

FCC employees and job applicants who file EEO complaints against the FCC provide PII to the FCC's Office of Workplace Diversity (OWD), which investigates the complaints. Individuals who have filed EEO complaints for investigation have implied consent.

Please see the list of the FCC's Privacy Impact Assessments for more information on how the FCC collects information from the public.

**E. Please explain how these PII data elements will be processed or used in the course of operating this information system.**

For a majority of FCC applications on ServiceNow, PII is not collected directly from the public. Except for two FCC applications built on the ServiceNow platform, any information provided by and pertaining to members of the public is incidentally stored. To the extent the incidental information is used, the use is ancillary to the FCC's enforcement, regulatory, licensing and other activities.

AULS tracks trouble tickets for members of the public experiencing problems with the FCC's electronic systems, or who have questions regarding filings with the FCC. The FCC collects contact information from these members of the public to respond to their inquiries. Occasionally, the FCC will collect tax ID numbers from members of the public through AULS to resolve registration problems with the system.

The EEO Complaint system is a repository for information related to EEO complaints against the FCC. OWD uses the information in the system to track and investigate complaints and respond to complainants, including FCC employees and job applicants.

Other FCC systems on the ServiceNow platform contain employee PII for internal operational, personnel, and security management at the agency.

**F. What steps will the FCC take to make sure this PII 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 parties providing the data to ensure the completeness, accuracy, and currency of data at the time it is created. Information that is used by the FCC as part of its 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., Communications Act, personnel laws, administrative or court evidentiary rules and procedures).

**G. Are there procedures in place to allow individuals access to their PII or to correct inaccurate information?**

To the extent any information in these FCC applications on ServiceNow are “records” under the Privacy Act of 1974, an individual may make a [request](#) for access to information the FCC maintains about her or him. The FCC’s Privacy Act Information page provides links to the [FCC’s System of Records Notices \(SORNs\)](#), as well as information about making [Freedom of Information Act \(FOIA\) requests](#) and the [online FOIA request form](#). Individuals seeking access must follow the FCC’s Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) at 47 C.F.R. § 0.551, et seq. Access to information under the Privacy Act is subject to certain exemptions.

**H. How long will the PII be retained and how will it be disposed of?**

Information in the FCC ServiceNow cloud instance is retained and destroyed in accordance with applicable FCC policies and procedures, as well as with the FCC records disposition schedule and General Records Schedules approved by the National Archives and Records Administration (NARA). FCC staff receive training and reminders about their records and destruction obligations. All information will be securely and irreversibly disposed of/destroyed in accordance with applicable FCC policies and procedures, OMB, NARA, and NIST regulations and guidelines.

## 1.4. Data Security

### A. Are there administrative procedures and technical safeguards in place to protect the data in the system? What controls are in place to ensure proper use of the data?

The FCC protects its information resources with a dynamic set of security measures. Some of these measures (e.g., network firewalls, physical security) protect the entire FCC enterprise, while other measures (e.g., user access restrictions, encryption) are applied to specific information systems. Following the risk-based policy established in the Federal Information Modernization Act (FISMA), the FCC applies more security measures (also known as security “controls”) to information systems that present higher operational risks. Consistent with this policy, the FCC applies specific security controls to systems that collect and process PII. A comprehensive list of the security and privacy controls the FCC may apply to its information systems can be found in National Institute of Standards and Technology (NIST) Special Publication No. 800-53 (revision 4), <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>.

The FCC purchases cloud computing services from providers that have been authorized under the Federal Risk and Authorization Management Program (FedRAMP). Cloud service providers that have received this authorization have demonstrated that they apply security controls to their computing resources in a manner that is consistent with the federal risk-based information security requirements the FCC follows.

### B. Has the system undergone the appropriate security risk assessment and received authority to operate?

Yes. Current Risk Assessment completed on May 17, 2019 and previous Authority to Operate received on December 20, 2017.

## 1.5. Access and Sharing of the Information

### A. Which FCC employees and contractors will have access to the PII in this information system?

Will Have Access	How and Why the Data Will be Accessed
FCC Staff	Access to ServiceNow is restricted to authorized FCC system owners and end users. All system owners and end users must adhere to the FCC Rules of Behavior. Access to the information stored within ServiceNow is dependent on the particular business purpose and the access permissions granted to a specific user. For example, system administrators may have access to system data and system audit logs in order to manage access roles, monitor system usage, perform system audits, and complete other necessary job functions.

Will Have Access	How and Why the Data Will be Accessed
Contractors	FCC may have contractor support within program areas, and these contractors will have access to the information in ServiceNow as required to perform their duties.
Office of Inspector General (OIG)	Under appropriate circumstances, data stored within ServiceNow or ServiceNow log data may be provided to the OIG for auditing or law enforcement purposes.

**B. Will the information be shared with 3<sup>rd</sup> parties as part of the operations of the information system (e.g., through an application programming interface or “API”)?**

Software as a service requires the service provider to have access to information collected and stored on its applications. Authorized FCC contractors have access to information in ServiceNow, when necessary. Some authorized FCC contractors have access to ServiceNow simply as users, and one or more authorized FCC contractors have access to certain administrative functions. All FCC contractors are required to complete security and privacy training prior to obtaining access to any FCC systems, and complete annual security and privacy training to maintain network access and access to those systems.

Contractors who access ServiceNow are subject to the same rules and policies as FCC staff. Contractors must also follow the reporting and other procedures in the FCC’s Breach Notification Policy.

**1.6. Privacy Act System of Records Notice**

**A. Is the FCC planning to publish or has it already published a Privacy Act System of Records Notice (SORN) for this information system? If the FCC has already published a SORN, please provide a citation to the Federal Register.**

The FCC is not required to publish a SORN for ServiceNow because it is not a system of records, as that term is defined the Privacy Act, 5 U.S.C. § 552a(a)(5).

## Appendix A - Acronyms and Abbreviations

[Populate based upon abbreviations used in the document. ]

**Table A-1: Acronyms and Abbreviations**

Acronym	Definition
AULS	Auctions and Universal Licensing System
EEO	Equal Employment Opportunity
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Modernization Act
FOIA	Freedom of Information Act
IaaS	Infrastructure as a Service
IPA	Initial Privacy Assessment
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OWD	Office of Workplace Diversity
PaaS	Platform as a Service
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SaaS	Software as a Service
SORN	System of Records Notice