UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT FOR ZENDESK

November 2021
Annual Review Date

OFFICE OF GENERAL COUNSEL

WASHINGTON, DC 20554

Next Review Cycle: November 2022

Record of Approval

Document Approval		
Drafter Name: Al R. Shipman		**Bureau/Office: OMD/IR**
SAOP Approval		
Printed Name: Margaret Drake		**Senior Agency Official for Privacy**
Signature: MARGARET DRAKE Digitally signed by MARGARET DRAKE Date: 2021.11.19 10:50:12 -05'00'	**Date**	

Record of Approval

Date	Description	Name
9/10/2021	Validation of information – System Owner	James Brown
9/24/2021	Validation of completeness – IT Compliance Lead	Liem Nguyen

Revision History

Date	Description	Name
5/26/2021	Original Document Created	ISSO/Privacy
8/16/2021	System Owner review and updates	James Brown
9/29/2021	1.2B Bureau names updated, PII Information updated, Accounting Information System summary added 1.3 Collected and updated data types 1.4C Updated the statement to the approved privacy summary 1.5B Updated the statement to approved privacy summary 1.6 Specific users added to each application	ISSO/Al Shipman

ZenDesk

1.1. Introduction

Section 208 of the E-Government Act of 2002[1] 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.*"[2]

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).

System owners, in collaboration with the Information System Security Officers (ISSOs) should complete the **Initial Privacy Assessment (IPA)** prior to filling out the PIA. The FCC Senior Agency Official for Privacy (SAOP) uses the IPA to determine whether a system will collect the kind of information that would make it subject to the requirements of Section 208, including a PIA. A PIA should not be completed until an IPA is completed and the SAOP makes a determination.

If you have any questions, please contact the Privacy Team at privacy@fcc.gov.

[1] 44 U.S.C. § 3501 note.

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

1.2. Authority To Operate (ATO) Boundary Overview

For each IT system that resides within the ATO Boundary, please use the table below to provide the system name, a brief description of the what the system does, whether it contains Personally Identifiable Information (PII) and a brief description of the PII (if applicable), the applicable System of Records Notice, the legal authorities to collect and maintain the PII, and whether the PII is shared with other systems (internal or external).

Please copy the table as necessary to complete the information for each system within the boundary.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Consumer Complaint Center (CCC)
NAME OF BUREAU Consumer & Governmental Affairs Bureau (CGB)
DOES THE SYSTEM CONTAIN PII? Yes. The PII is retrieved by ticket ID or email address.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) PII from consumers filing informal consumer complaints with the Commission, which include their name, home address, phone number, and email address.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? FCC/CGB-1, Informal Complaints, Inquiries, and Requests for Dispute Assistance
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The Commission is authorized to request this information from consumers under Sections 1, 4, 206, 208, 225, 226, 227, 228, 255, 258, 301, 303, 309(e), 312, 362, 364, 386, 507, 710, 713, 716, 717, and 718 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154, 206, 208, 225, 226, 227, 228, 255, 258, 301, 303, 309(e), 312, 362, 386, 507, 610, 613, 617, 618, and 619; Sections 504 and 508 of the Rehabilitation Act, 29 U.S.C. 794 and 794d; and 47 CFR 0.111, 0.141, 1.711 et seq., 14.30 et seq., 20.19, 64.604, 68.414 et seq., and 79.1 et seq..
Does the system leverage the FCC's Accounting for Disclosure control (Access to the Information)? Yes. The Privacy Team keeps an accurate accounting of disclosures of information
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes. PII is shared with ServiceNow, Socrata and EBATS.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Public Safety Support Center (PSSC)
NAME OF BUREAU Public Safety and Homeland Security Bureau (PSHSB)
DOES THE SYSTEM CONTAIN PII? Yes. The PII is retrieved by ticket ID or email address.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) PII from public safety entities and individuals filing complaints and inquiries with the Commission. PII that is collected includes name, mailing address, email address, and phone number, as well as business contact information.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? FCC/PSHSB-1 – FCC Emergency and Continuity Alerts and Contacts System, and FCC/PSHSB-2 – PSHSB Contact Database
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The Commission is authorized to request this information from consumers under Sections 1, 4, 206, 208, 225, 226, 227, 228, 255, 258, 301, 303, 309(e), 312, 362, 364, 386, 507, 710, 713, 716, 717, and 718 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154, 206, 208, 225, 226, 227, 228, 255, 258, 301, 303, 309(e), 312, 362, 386, 507, 610, 613, 617, 618, and 619; Sections 504 and 508 of the Rehabilitation Act, 29 U.S.C. 794 and 794d; and 47 CFR 0.111, 0.141, 1.711 et seq., 14.30 et seq., 20.19, 64.604, 68.414 et seq., and 79.1 et seq..
Does the system leverage the FCC's Accounting for Disclosure control (Access to the Information)? Yes, The Privacy Team keeps an accurate accounting of disclosures of information
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Administrative Services Center (ASC)

NAME OF BUREAU Office of Managing Director (OMD)
DOES THE SYSTEM CONTAIN PII? Yes. The PII is retrieved by ticket ID or email address.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) PII from FCC employees requesting administrative services consists of an email address
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? FCC-2, Business Contacts and Certifications
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The Commission is authorized to request this information from consumers under Sections 1, 4, 206, 208, 225, 226, 227, 228, 255, 258, 301, 303, 309(e), 312, 362, 364, 386, 507, 710, 713, 716, 717, and 718 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154, 206, 208, 225, 226, 227, 228, 255, 258, 301, 303, 309(e), 312, 362, 386, 507, 610, 613, 617, 618, and 619; Sections 504 and 508 of the Rehabilitation Act, 29 U.S.C. 794 and 794d; and 47 CFR 0.111, 0.141, 1.711 et seq., 14.30 et seq., 20.19, 64.604, 68.414 et seq., and 79.1 et seq..
DOES THE SYSTEM LEVERAGE THE FCC'S ACCOUNTING FOR DISCLOSURE CONTROL (ACCESS TO THE INFORMATION)? Yes, The Privacy Team keeps an accurate accounting of disclosures of information
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No

A. Is this a new ATO Boundary or an existing ATO Boundary?

☐ New Boundary

☒ Existing Boundary

B. If the ATO Boundary is/will consist of cloud-based computing system(s),[3] please check the box that best describes the service the FCC receives/will receive from the cloud computing provider:

[3] *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 applications on the provider's cloud network (Software as a Service or SaaS).

- Consumer Complaint Center (CCC) – The CCC, which allows consumers to submit informal consumer complaints online, is a ticketing system for FCC staff to process complaints and serve complaints on regulated entities, and to track calls into the FCC's toll free 888-CALL-FCC number. The CCC ticketing system used by the public to submit tickets that are reviewed and processed by FCC staff in the Consumer and Government Affairs Bureau (CGB).

  The CCC allows callers to submit complaints related to telecommunications issues, including television, phone, internet, and radio. When the complaint submitted to the CCC is about a telecom billing or service issue, the FCC generally serves the complaint on the provider. Other complaints are shared internally to inform policy and potential enforcement activities. When retrieving the consumers' information, FCC CGB staff will search and retrieve the information by the supplied email address and/or ticket ID.

- Public Safety Support Center (PSSC) - The PSSC allows public safety-related entities and individuals to submit requests online through a ticketing system that FCC staff use to process the requests. The PSSC also allows the public to submit feedback on alerting tests. The PSSC ticketing system is used by the public to submit tickets that are reviewed and processed by FCC staff in the Public Safety and Homeland Security Bureau (PSHSB)

  The PSSC handles alerting feedback, notifications of service outages, and complaints related to carrier provision of location information. PSSC also register issues or submit inquiries regarding a primary Public Safety Answering Point (PSAP), Public Safety operations, or FCC rules and regulations. When retrieving the consumers' information, FCC PSHSB staff will search and retrieve the information by the supplied email address and/or ticket ID.

- Administrative Services Center (ASC) - The ASC allows internal FCC staff to submit requests for issues related to building/property management, and a ticketing system for FCC Administrative Operations (AO) staff to process the requests. The ASC ticketing system is used by FCC staff to submit tickets that are reviewed and processed by FCC AO staff. When retrieving FCC staff information, FCCAO staff will search and retrieve the information by the

supplied email address and/or ticket ID if available.

☐ The FCC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service or PaaS) [list applicable system(s)]

☐ 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) [list applicable system(s)]

C. **If the IT systems in the ATO Boundary are in the cloud, are they FedRAMP certified?**

☒ Yes, all the IT systems are FedRAMP certified
☐ No, none, or only some, of the IT systems are FedRAMP certified

Zendesk became FedRAMP certified in 2020.

1.3. Collection of Data

A. Please explain why it is necessary to collect PII to carry out the purpose of each of the system(s) that maintain PII within this Boundary.

The collected PII data in the Zendesk Boundary is necessary because:
Consumer Complaint Center:
It is necessary to collect PII from consumers for **CGB** to assist in the resolution of their informal consumer complaint and to provide the PII to carriers to the extent necessary to permit them to identify their customers and resolve informal complaints.

Public Safety Support Center:
It is necessary to collect PII from public safety entities and individuals for **PSHSB** to assist in the resolution of their inquiry or complaint.

Administrative Services Center:
It is necessary to collect PII from Commission employees to assist in the resolution of their administrative request.

B. For each system within this Boundary, will this PII be collected from individuals themselves, or from third parties? If collected from individuals themselves, link to the

Privacy Act Statement[4] for each system that is included with the online or paper form the system(s) use(s) to collect the PII.

Consumer Complaint Center:
PII will be collected from individuals. Below is the link to the Privacy Act Statement that is included at the top of the consumer complaint forms.
https://www.fcc.gov/general/fcc-notice-required-privacy-act

Public Safety Support Center:
PII will be collected from individuals and third parties. [It does not look like there is a Privacy Statement.]

Administrative Services Center:

PII will be collected from individuals.

C. What steps is the FCC taking to limit the collection of PII to only that which is necessary?

Consumer Complaint Center:
The forms on the Consumer Complaint Center are limited to information necessary to address complaints and include drop downs and formatted fields.

Public Safety Support Center:
The forms on the Public Safety support Center are limited to contact information necessary to address complaints and inquiries.

Administrative Services Center:
The forms on the Administrative Services Center are limited to contact information necessary to resolve administrative requests.

What steps will the FCC take to make sure this PII is accurate, complete, and up to date?

It is the responsibility of the parties providing the data to ensure the completeness and accuracy of the data at the time it is entered into the system.

[4] A Privacy Act Statement must inform individuals about (1) the authority to solicit information, (2) the principal purpose(s) for collecting the information, (3) the routine uses for disclosing the information, and (4) whether providing the information is mandatory or voluntary.

1.4. Use of the Data

A. Please explain the data flow, including whether the PII will be ingested from, or shared with, another system. Are internal connections reflected in the Cyber Security Asset Management tool (CSAM)? Are Information Sharing Agreements (ISAs) in CSAM for external connections?

Data from the CCC is extracted nightly and stored internally in ServiceNow. From ServiceNow, some of the data is pushed to EBATS or Socrata. There are no external connections for Zendesk.

B. Will the information be shared with third parties as part of the operations of the information system (e.g., through an application programming interface or "API")?
No

C. How long will the PII be retained and how will it be disposed of?
Information in the systems within this boundary is retained and destroyed in accordance with applicable FCC policies and procedures, as well as with the FCC records disposition schedule or General Records Schedules approved by the National Archives and Records Administration (NARA).

1.5. Data Security and Privacy

A. What are the system's ratings for confidentiality, integrity, and availability?

Confidentiality	**__High**	**_X_Moderate**	**___Low**
Integrity	**__High**	**_X_Moderate**	**___Low**
Availability	**__High**	**_X_Moderate**	**___Low**

Boundary rating is "Moderate". Refer to boundary's FIPS 199 dated May 10, 2021 for their ratings.

B. Discuss the physical, administrative, and technical controls in place to protect the data in the system.

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 5 [NIST].

C. Does the system inherit privacy controls from an external provider? If an Interconnection Security Agreement (ISA) , Memorandum of Understanding (MOU) , or similar document is in place, please summarize the privacy applicable portions of the document.

No.

1.6. Access to the Information

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

Consumer Complaint Center:
Certain employees and contractors in CGB have access as part of their job duties to support the informal consumer complaint process. In addition, a limited number of employees in the Enforcement Bureau (EB) have read-only access to complaint data as well as a few employees in other bureaus.

Public Safety Service Center:
Certain employees and contractors in PSHSB have access as part of their job duties to address the issues raised.

Administrative Services Center:
Certain employees and contractors in ASC have access as part of their job duties to address the issues raised.

B. Does this system leverage Enterprise Access Controls?

Yes