UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT (PIA) FOR THE BROADBAND DATA COLLECTION (BDC)

November 2023

OFFICE OF GENERAL COUNSEL

Washington DC, 20554

Next Review Cycle: November 2024

Record of Approval

Document Approval	
Drafter Name: C. Jason Happ	**Bureau/Office:** OEA
SAOP Approval	
Printed Name: Elliot S. Tarloff	**Senior Agency Official for Privacy**
Signature & Date ELLIOT TARLOFF Digitally signed by ELLIOT TARLOFF Date: 2023.12.21 14:36:48 -05'00'	

Record of Approval

Date	Description	Author
01/05/2022	[2022 Template] Validation of information – System Owner	Jonathan McCormack
01/24/2022	[2022 Template] Validation of completeness – IT Compliance Lead	Liem Nguyen
02/09/2022	[2022 Template] Final review and approval – Privacy	Linda Oliver, SAOP
12/07/2023	Validation of Accuracy – System Owner	Jonathan McCormack
12/18/2023	Validation of Completeness – IT Compliance Lead	Shelton Rainey

Revision History

Date	Description	Name
8/10/2021	[2022 Template] Original Document Created	C. Jason Happ, Cybersecurity Specialist, Emprata
01/11/2022	[2022 Template] BDC Inputs incorporated to template	C. Jason Happ Hans Agarwal, FCC Security and Compliance
01/14/2022	[2022 Template] 1.2: Authority to Operate (ATO) Boundary Overview -> PII descriptions updated 1.3: Collection of Data -> Further refined technical descriptions 1.4: Use of Data -> Incorporated further details to enhance understanding for individuals lacking contextual details	C. Jason Happ Elliot Tarloff, FCC Attorney Advisor Jonathan McCormack, Acting BDC System Owner
01/25/2022	[2022 Template] BDC Template update with ISSO Contractor and Compliance Lead	Liem Nguyen, Hans Agarwal
1/27/2022	[2022 Template] Edits to 1.2 list of PII, and 1.6b list of Enterprise Access Controls	Elliot Tarloff Jonathan McCormack

Date	Description	Name
2/8/2022	[2022 Template] Edits to .3c and 1.6b	Elliot Tarloff at direction of Linda Oliver, acting SAOP
8/23/2023	Transposition of BDC inputs into new template provided by the FCC Cybersecurity and Compliance Team (Alexander Egorov); review and incorporation of additional details	C. Jason Happ, Cybersecurity Specialist, Emprata
10/10/2023	Revisions by Privacy Team to Sections 1.2, 1.3A-D, 1.4A-B, 1.5A	Privacy Advisor – Katherine Morehead Senior Agency Official for Privacy (SAOP) – Elliot S. Tarloff
10/27/2023	Formatting edits and revisions to Sections 1.2, 1.3B, 1.4A-B	SAOP
11/2/2023	Clerical edits	SAOP
11/9/2023	Final formatting review	C. Jason Happ, Cybersecurity Specialist, Emprata

BDC System Boundary

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).

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Broadband Data Collection (BDC). This PIA encompasses only the BDC and not systems that transmit data to, or receive data from, the BDC through challenge and crowdsource processes, which may include the ESI Cloud SaaS-2 boundary (ZenDesk), the FCC Speed Test App, and the FCC Enterprise Data Platform, which is part of the FCC Enterprise Support Cloud Infrastructure – IaaS boundary.
NAME OF BUREAU Office of Economics and Analytics (OEA)
DOES THE SYSTEM CONTAIN PII? Yes. BDC System Administrators are able to search and retrieve challenge records for purposes of administering the challenge and crowdsource processes.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) The BDC collects PII from individuals—which information can include names, location information, contact information, device information, and network/connection information—to facilitate challenge and crowdsource processes.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? FCC/OEA-6
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The FCC is collecting, maintaining, using, and sharing the PII pursuant to the requirements of the Broadband Deployment Accuracy and Technological Availability Act (Broadband DATA Act), Pub. L. No. 116-130, § 806(b), 134 Stat. 228, 238 (2020), amended by Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, § 60102(h)(2)(E)(ii), 135 Stat. 429, 1198 (2021) (codified at 47 U.S.C. § 646(b)).
DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT? Yes. The Privacy Team keeps an accurate accounting of disclosures of information.

DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS?

Yes.

(1) The BDC receives data, including PII, from the FCC SpeedTest App, which is maintained by a third-party contractor under separate authorization; the BDC is also designed to receive data from other authorized third-party speed-test applications.

(2) The BDC may be upgraded to support the exchange (transmission to and receipt from) information, including PII, with the FCC ESI Cloud SaaS-2 Boundary (ZenDesk). Such data exchanges would facilitate tracking and resolution of challenges.

(3) The BDC transmits data to the FCC Enterprise Support Cloud Infrastructure – IaaS, boundary. Specifically, data are transmitted to the FCC Enterprise Data Platform, which is an enterprise-level data warehouse for archiving, analysis, and reporting, which ingests data from the BDC's dedicated AWS Redshift database.

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:

☐ The FCC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS) [list applicable system(s)]

☐ 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) [BDC]

[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.

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

☐ Not applicable, ATO boundary is not Cloud based.

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.

Certain PII must be collected for the BDC challenge process to operate as intended. Specifically, the BDC collects broadband availability data from fixed and mobile broadband service providers. Consumers and other authorized entities provide feedback on availability and quality via the BDC challenge and crowdsource processes. To properly coordinate and adjudicate these challenges, certain PII elements need to be collected from individuals who participate in the challenge and crowdsource processes.

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.

The BDC system collects information from the following external sources:

- Fixed and mobile providers: Broadband providers across the nation that will be providing granular availability data, supplemental information and challenge responses.
- Government Entities: Includes state and local governments and government agencies that are primarily responsible for mapping or tracking broadband access service coverage, as well as governmental entities submitting challenge and crowdsource information.
- Tribal Entities: Includes Tribal governmental entities that are primarily responsible for mapping or tracking broadband access service coverage, as well as Tribal entities submitting challenge and crowdsource information.
- Third Parties: Outside parties capable of submitting verified broadband availability data, if the FCC determines it is in the public interest to use their data, as well as third parties submitting challenge and crowdsource data.

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.

- Consumers: Includes members of the general public that will view the broadband availability information on the public broadband maps and submit fixed, mobile, or fabric challenges. Consumers may also download and submit results via the FCC Speed Test App or other approved third-party speed test app that shares results with the FCC.
- Broadband Serviceable Location Fabric Contractor(s): Entities responsible for creating and delivering the Broadband Serviceable Location Fabric data, to include an initial submission and periodic updates.
- Federal Agencies: Federal Agencies submit funding data, which is aggregated with the aforementioned data sources so that users are able to search and filter federal funding programs by specific ISPs receiving funding, the duration timeline, the number of locations included in the project and the download and upload speeds.

PII is collected directly from individuals who choose to participate in the challenge and crowdsource processes. The Privacy Act Statement is as follows:

PRIVACY ACT STATEMENT

The information collected in this system, including name, street address, phone number(s), email address, geolocation information, timestamps, IP addresses, and other mobile device specifications, is used by the FCC for the purposes of collecting, disseminating, and mapping broadband availability data, collecting crowdsourced and challenge data, and conducting the crowdsourced and challenge processes. Information contained in this system may be made available to other individuals and entities when necessary and appropriate to implement the Broadband Data Collection, and for other routine purposes. For more information about how your information may be used, please review the BDC Privacy Act Statement.

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

The mechanisms used by the BDC to collect data for the challenge and crowdsource processes limit the collection to include only names, and certain location information, contact information, device information, and network/connection information, which are necessary to properly coordinate and adjudicate challenges.

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

It is the responsibility of individuals participating in the challenge and crowdsource processes to ensure the completeness and accuracy of the data at the time those data are entered into the system. Further, the BDC relies on third party vendors, including the FCC Speed Test App, to accurately collect device and network/connection geolocation information. Once PII is ingested into the BDC, data integrity, including of PII, is controlled through user access safeguards and annual data validation testing (i.e., contingency planning exercises).

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?

There are three types of challenges (which require the submission of PII) that can be initiated through the BDC: Fixed Broadband, Mobile Broadband, and Broadband Serviceable Location Fabric challenges.

Fixed Broadband:
Users can challenge whether a fixed broadband provider offers service at a particular address by submitting a challenge directly into the BDC—either via the BDC Filer Interface, for authenticated filer bulk challenges, or via the Broadband Map Interface, for individual consumer challenges. The challenge data and evidence are stored in a database within the FCC's BDC system, which is hosted by AWS. Therefore, all information at rest will be protected by the AWS/ FCC Enterprise Support Cloud Infrastructure-IaaS (AWS) boundary group. The FCC monitors the fixed broadband challenges through resolution. Once resolved, the consumer receives an email with the resolution and status update.

Mobile Broadband:
Consumers have the ability to download the FCC's Speed Test App (maintained by a contractor under separate authorization) to provide actual measurements on mobile broadband speeds and other metrics. The data collected by the Speed Test App, which includes PII, are transmitted to a database managed by the FCC Speed Test App contractor. The contractor transmits speed test data to the BDC via a data transmission initiated by an automated API process. Upon receiving the speed test data, the FCC Office of Engineering and Technology (OET) subjects the data to proprietary algorithms to confirm the validity of the challenge. If the challenge is valid, it is maintained in the BDC, and notice is sent to the relevant Mobile Provider and consumer of the challenge location and details.

Broadband Serviceable Location Fabric:
Consumers can challenge data in the Broadband Serviceable Location Fabric ("Fabric"), which is a database of all locations to which broadband service is or could be provided. These challenges are submitted either via the BDC Filer Interface, for authenticated filer bulk challenges, or via the Broadband Map Interface, for individual consumer challenges The FCC relies on the Fabric when ingesting and publishing fixed broadband availability data. After a consumer provides his/her contact information, information about a location that he/she believes is incorrect or missing, and justification, the challenge data and are stored in a database within the FCC's BDC system, which is hosted by AWS. The

FCC monitors the challenge through resolution. Once resolved, the consumer will receive an email with the resolution and status update.

The internal connections are reflected in the architectural diagrams contained within the System Security Plan (SSP), which is stored within CSAM. If required, Information Sharing Agreements (ISA) will be implemented, and reflected in CSAM, prior to sharing non-public, PII, or other sensitive data from the BDC. There are currently no use cases contemplated in the design of the BDC where such data would be shared with external systems.

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")?

The BDC collects data, including PII, from a third party (i.e., the FCC Speed Test App vendor) via API, and the BDC is designed to collect data, including PII, from other authorized, third-party speed test applications. The BDC is also designed to share data, including PII, via API but only with other FCC boundaries.

There are currently no uses cases contemplated in the design of the BDC where data would be disclosed to other third-party systems via API. But there are instances where data from the BDC would be shared with third parties as part of the operations of the BDC. Specifically, these are noted in the "Routine Uses" section of the BDC Privacy Act Statement:
Privacy Act Statement | Federal Communications Commission (fcc.gov).

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	☒ Moderate	☐ Low
Integrity	☐ High	☒ Moderate	☐ Low
Availability	☐ High	☒ Moderate	☐ Low

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.

Yes, the BDC inherits certain privacy controls from other FCC-Enterprise boundaries, as noted below.

(1) ESI Cloud – IaaS
(2) ESI Cloud - PaaS
(3) ESI Cloud – SaaS Enclave 2
(4) Enterprise Identity
(5) Enterprise Support Infrastructure

1.6 Access to the Information

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

Certain FCC employees and contractors will have access to the PII in the BDC system based upon their business need and user role in the system. Specifically, the following user roles will have access to PII:

- System Administrators
- System Analysts
- Challenge Adjudicators
- Filer Support Technician
- BDC Challenge Administrator

*Refer to the BDC Access Control Policy (ACP) for further details regarding the roles listed here.

B. Does this system leverage Enterprise Access Controls?

Yes

- Okta for external users and administrators
- Filer-managed API keys for authenticated users' programmatic / API access to filer interface
- Administrator-managed API keys for approved third-party systems' programmatic / API access to challenge data submissions
- Data.gov API keys for public users' programmatic / API access to map interface