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

February 2022

OFFICE OF GENERAL COUNSEL
Washington DC, 20554
## Record of Approval

### Document Approval

<table>
<thead>
<tr>
<th>Drafter Name:</th>
<th>Jason Happ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bureau/Office:</td>
<td>OEA</td>
</tr>
</tbody>
</table>

### SAOP Approval

<table>
<thead>
<tr>
<th>Printed Name:</th>
<th>Linda Oliver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acting Senior Agency Official for Privacy:</td>
<td>Linda L. Oliver</td>
</tr>
<tr>
<td>Signature:</td>
<td>Digitally signed by Linda L. Oliver</td>
</tr>
<tr>
<td>Date</td>
<td>2022.02.09 16:47:40 -05'00'</td>
</tr>
</tbody>
</table>

## Record of Approval

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/05/2022</td>
<td>Validation of information – System Owner</td>
<td>Jon McCormack</td>
</tr>
<tr>
<td>01/24/2022</td>
<td>Validation of completeness – IT Compliance Lead</td>
<td>Liem Nguyen, IT Compliance Lead</td>
</tr>
</tbody>
</table>

## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/10/2021</td>
<td>Original Document Created</td>
<td>Jason Happ, Cybersecurity Specialist, Emprata</td>
</tr>
<tr>
<td>01/11/2022</td>
<td>BDC Inputs incorporated to template</td>
<td>Jason Happ, Hans Agarwal, FCC Security and Compliance</td>
</tr>
<tr>
<td>01/14/2022</td>
<td>1.2: Authority to Operate (ATO) Boundary Overview -&gt; PII descriptions updated</td>
<td>Jason Happ, Elliot Tarloff, FCC Attorney Advisor</td>
</tr>
<tr>
<td></td>
<td>1.3: Collection of Data -&gt; Further refined technical descriptions</td>
<td>Jonathan McCormack, Acting BDC System Owner</td>
</tr>
<tr>
<td></td>
<td>1.4: Use of Data -&gt; Incorporated further details to enhance understanding for individuals lacking contextual details</td>
<td></td>
</tr>
<tr>
<td>01/25/2022</td>
<td>BDC Template update with ISSO Contractor and Compliance Lead</td>
<td>Liem Nguyen, Hans Agarwal</td>
</tr>
<tr>
<td>1/27/2022</td>
<td>Edits to 1.2 list of PII, and 1.6b list of Enterprise Access Controls</td>
<td>Elliot Tarloff, Jonathan McCormack</td>
</tr>
<tr>
<td>2/8/2022</td>
<td>Edits to 1.3c and 1.6b</td>
<td>Elliot Tarloff at direction of Linda Oliver, acting SAOP</td>
</tr>
</tbody>
</table>
BDC System Boundary

1.1. Introduction

Section 208 of the E-Government Act of 2002 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.*”

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.

---


2. OMB Memorandum No. M-03-22 (Sep. 26, 2003),
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.

<table>
<thead>
<tr>
<th>INFORMATION ABOUT THE SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME OF THE SYSTEM</td>
</tr>
<tr>
<td>NAME OF BUREAU</td>
</tr>
<tr>
<td>DOES THE SYSTEM CONTAIN PII?</td>
</tr>
</tbody>
</table>
| PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) | The following PII Elements could be collected via the BDC through this challenge process:  
- Full Name  
- Home Address  
- Phone Number(s)  
- Email Address  
- Geolocation Information  
- User ID  
- TCP / IP Information  
- Other – Mobile device information (e.g., make, model, operating system, IMEI)  
- Other – Timestamp |
| IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? | FCC/WCB-4: Consumer Challenge Process |
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII?


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.

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

☒ New Boundary
☐ Existing Boundary

A. If the ATO Boundary is/will consist of cloud-based computing system(s), 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) [list applicable system(s)- Amazon Web Service (AWS)]

---

B. **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

*Note: The BDC is hosted on the FCC instance of AWS, which is FedRAMP certified. The BDC application is not FedRAMP certified.*

### 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 BDC Boundary is necessary because: Certain PII is required 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 process. To properly coordinate and adjudicate these challenges, certain PII data elements need to be collected.

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 for each system that is included with the online or paper form the system(s) use(s) to collect the PII.**

PII will be collected from individuals, including through the FCC Speed Test App, built by a third-party vendor that includes an option for consumers to provide challenges in the BDC system. The Privacy Act Statement will appear at the point of collection.

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 process are limited to include only name, address, phone number, email address, and User ID, as well as device identification, TCP/IP, time, and geo-location data 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 the customers providing contact data to ensure the completeness and accuracy of the data at the time it is entered into the system. Further, the BDC relies on third party vendors, including the FCC Speed Test App, to accurately collect device identification, TCP/IP, time and geolocation information. Once PII data is ingested to 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?

PII is being provided by consumers into ZenDesk as part of the challenge process. There are three types of challenges 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 point. After providing their contact information and justification in ZenDesk, an official ticket is created in ZenDesk, along with a unique ticket number. The challenge data and associated ticket number 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 ticket through resolution. Once resolved, the consumer will receive an email via ZenDesk with the resolution and status update.

**Mobile Broadband:**

Consumers have the ability to download the FCC’s Speed Test App (not a part of the BDC) to provide actual measurements on mobile broadband speeds and other metrics. The data collected by the Speed Test App can be transmitted to a database managed by the FCC Speed Test App vendor. The vendor transmits speed test data to the BDC via a data transmission initiated by an automated API process.
Upon receiving the speed test data, it will be subject to algorithms developed by the FCC’s Office of Engineering and Technology (OET) to confirm the validity of the challenge. If the challenge is valid, a ZenDesk ticket is created automatically by the BDC to notify the 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. 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 BDC creates an official ticket in ZenDesk, along with a unique ticket number. The challenge data and associated ticket number 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 ticket through resolution. Once resolved, the consumer will receive an email via ZenDesk) 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”)?**

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?

<table>
<thead>
<tr>
<th></th>
<th>High</th>
<th>Moderate</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>___</td>
<td>X__</td>
<td>___</td>
</tr>
<tr>
<td>Integrity</td>
<td>___</td>
<td>X__</td>
<td>___</td>
</tr>
<tr>
<td>Availability</td>
<td>___</td>
<td>X__</td>
<td>___</td>
</tr>
</tbody>
</table>

Boundary rating is “Moderate.” Refer to the BDC FIPS 199 for 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 (SP) No. 800-53, Revision 5 [NIST]. Finally, the BDC resides within the FCC instance of AWS, which is FedRAMP accredited, and any customer responsibility controls are addressed through NIST SP No. 800-53.

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?**

   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

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

   *Note: API access to challenge data submissions for approved third parties will not disclose any non-public PII components of the submitted challenge data.*

c. **Does the system leverage the FCC’s Accounting for Disclosure control?**

   Yes, the Privacy Team keeps an accurate accounting of disclosures of information.