UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT (PIA) FOR THE FCC SPEED TEST SYSTEM

MARCH 2024

OFFICE OF GENERAL COUNSEL

45 L Street, NE Washington DC, 20554

Next Review Cycle: MARCH 2025

Record of Approval

Document Approval	
Drafter Name: C. Jason Happ	**Bureau/Office:** Office of Engineering and Technology (OET)
SAOP Approval	
Printed Name: Elliot S. Tarloff	**Senior Agency Official for Privacy**
X ELLIOT TARLOFF Digitally signed by ELLIOT TARLOFF Date: 2024.03.22 15:55:54 -04'00' **Signature & Date**	

Record of Approval

Date	Description	Author
03/22/2024	Validation of Accuracy – System Owner	Sean Yun
03/21/2024	Validation of Completeness – IT Compliance Lead	Shelton Rainey

Revision History

Date	Description	Name
12/07/2023	[2022 Template] Original Document Created; FCC Speed Test Platform inputs.	C. Jason Happ, Cybersecurity Specialist, Mozark
01/18/2024	Updated content to include the FCC Speed Test System, rather than just the platform and infrastructure components.	C. Jason Happ, Cybersecurity Specialist, Mozark
03/04/2024	Clerical/formatting edits and revisions to Sections 1.2, 1.3A-D, 1.4A, 1.5B	Privacy Advisor – Katherine Morehead Senior Agency Official for Privacy (SAOP) – Elliot S. Tarloff
03/15/2024	Updated FCC Speed Test System inputs to address SAOP comments.	C. Jason Happ, Cybersecurity Specialist, Mozark
3/19/2024	Accepted edits and final formatting edits	SAOP
3/22/2024	Accepted revisions to sections 1.3A, 1.3D, 1.4A, and 1.6A from COR.	SAOP

FCC Speed Test System, Part of Office of Engineering and Technology 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 FCC Speed Test System: Speed Test Mobile Application, Speed Test Servers, AWS Platform/Infrastructure.
NAME OF BUREAU Office of Engineering and Technology (OET)
DOES THE SYSTEM CONTAIN PII? Yes, the FCC Speed Test System contains PII. The FCC Speed Test System does not routinely retrieve speed test records based on name or other unique identifier.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Through the App, the FCC Speed Test System collects contact information and consent from users. Use of the app also triggers the collection of network, device, and location information.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? The Speed Test System is not a system of records, but when data originating from the Speed Test System are ingested to the BDC, they become records in the FCC/OEA-6 system of records.
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? Not Applicable.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes. The FCC Speed Test Application transmits PII data via secure API to the FCC's BDC. Please see the Interconnection Security Agreement (ISA) between the FCC and Mozark

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 Speed Test System – Infrastructure (AWS), was established on a FedRAMP-Accredited AWS instance, which is implemented and maintained by Mozark.

☐ 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)

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

The AWS Infrastructure that ingests PII from citizen-user devices is a FedRAMP certified AWS Platform. However, the FCC Speed Test Mobile Application is a custom-developed application for the FCC. Further, all of the Test Servers that communicate with the mobile app are either FedRAMP certified AWS servers or FedRAMP certified GCP servers.

*Note: In the future, there could be other third-party test servers for localities where FedRAMP certified AWS or GCP are not available, however, no PII is being passed through these servers.

☐ Not applicable, ATO boundary is not Cloud based.

[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.

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 FCC Speed Test System is designed to collect information on the availability and quality of mobile broadband and Wi-Fi services from consumers and authorized entities. To ensure high quality data and allow for the proper adjudication of challenges, the Speed Test System must collect certain PII data elements as set forth in Commission orders, *e.g.*, *Establishing the Digital Opportunity Data Collection Modernizing the FCC Form 477 Data Program*, Third Report and Order, 36 FCC Rcd 1126 (2021), and regulations, 47 CFR 1.7006(b)(1)(i), (e)(1)(i), for the Broadband Data Collection.

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.

PII will be collected from individuals through the FCC Speed Test Mobile Application. To that end, a Privacy Act Statement or another privacy notice will appear at the point of collection, within the FCC Speed Test Mobile Application.

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

The FCC Speed Test System is ingesting only the specific PII elements that the FCC has identified in their requirements to Mozark, which in turn are based on the requirements established in the FCC's BDC orders and regulations.

Mozark has provided configuration information to the FCC in the form of screen captures and other configuration files to validate that only the minimum required PII is being collected with respect to the requirements provided by FCC.

To that end, the PII data collected are limited to contact information, device information, geo-location, timestamp of the test conducted, and key network parameters.

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

The FCC Speed Test System relies on the FCC Mobile Speed Test Application to collect the data. It is the responsibility of App users to provide accurate contact 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.

consistent with BDC rules, users must certify within the Speed Test App that "To the best of my actual knowledge, information and belief, all statements provided are true and correct." The data are further assessed for compatibility with the BDC once they are ingested into the Speed Test System's AWS servers, before delivery to the FCC BDC. The FCC will evaluate challenge data through routine BDC processes, that may involve assessment of the accuracy, completeness, and timeliness of the data provided through the Speed Test System.

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?**

The primary data flow is as follows:

(1) Users input data, including PII, to the FCC Speed Test Mobile Application. Users also provide their consent for the FCC Speed Test Mobile Application to collect the information provided.

(2) Once a user initiates a test via the FCC Speed Test Mobile Application, the app transmits a test signal to the nearest Test Server. The "test signal" is a lightweight packet of information designed to quickly travel to the server and back, enabling the measurement of Round Trip-Time (RTT) or latency. The test signal does not contain any PII.

(3) User inputs, including PII, and performance data are aggregated by the FCC Speed Test Mobile Application, which securely transmits the data to the FCC Speed Test AWS Platform.

(4) Data within the FCC Sped Test AWS Platform are periodically securely transmitted to the BDC via an Application Programming Interface (API).

(5) All connections are reflected in CSAM.

(6) ISAs will be maintained in CSAM, once authorized.

There are two additional data flows. First, the PII that users input into the app is saved to the AWS platform; it is not stored on the phone. So when a user opens the app on subsequent occasions, the AWS platform is queried for the stored PII data and transmitted back from the cloud to the user's device. Second, a user's test results, including the PII collected, is available for data export from within the app to the local file system of the user's phone, after which, the user may use the data for any purpose.

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 FCC Speed Test System will transmit data via API to the FCC’s BDC and to no other entities.

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).The PII data will be retained for a duration of three years.

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.

At the direction of the FCC, Mozark has protected the Speed Test System with a dynamic set of security measures. Some of these measures (e.g., network firewalls, physical security) protect the entire 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), more security measures (also known as security “controls”) apply to information systems that present higher operational risks, and specific security controls apply to systems that collect and process PII. A comprehensive list of the security and privacy controls that may apply to the Speed Test System can be found in National Institute of Standards and Technology (NIST) Special Publication No. 800-53, Revision 5 [NIST]. Multi-factor authentication is used to control access. Appropriate encryption is used to cover the data at rest. The services themselves are hosted on AWS US East (N. Virginia) region which is FedRAMP Moderate accredited.

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 FCC Speed Test System inherits certain privacy controls from their AWS Platform-as-a-Service (PaaS) provider. Specifically, the FCC Speed Test Application relies upon the AWS FedRAMP accredited platform.

1.6 Access to the Information

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

Only the server administrator of Mozark has general access to the PII. There are no FCC employees that will have general access to the information within the FCC Speed Test Platform. However, the COR may request custom reports which can include user PII. Additionally, the data collected by the app are transmitted to the BDC, where certain employees and contractors will have access to the PII in the BDC system based upon their business need and user role in the system.

B. Does this system leverage Enterprise Access Controls?

Yes. Among other controls at the enterprise level, Mozark relies on the following:
(1) Office 365–based SSO for admin logins to the cloud system;
(2) API keys for communication between mobile and cloud system; and
(3) Administrator managed keys for cloud system access