UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT FOR REASSIGNED NUMBERS DATABASE (RND) BOUNDARY

December 10, 2021

OFFICE OF GENERAL COUNSEL

WASHINGTON, DC 20554

Record of Approval

Document Approval		
Privacy POC		
Printed Name: Kimberly Miller		**Senior Corporate Counsel, Somos, Inc**
Approval Structure		
Printed Name: Linda Oliver		**Associate General Counsel and Acting SAOP**
Signature: Linda L. Oliver Digitally signed by Linda L. Oliver Date: 2021.12.10 14:57:33 -05'00'	**Date**	

Record of Approval

Date	Description	Name
12/08/2021	Validation of information – System Owner (FCC)	Rebecca A. Maccaroni
12/10/2021	Validation of information – System Owner (Somos)	Beth Sprague, Somos, Inc.
12/08/2021	Validation of completeness – IT Compliance Lead	Liem Nguyen

Revision History

Date	Description	Name
04/01/2021	Original Draft Created	Kimberly Miller, Somos, Inc.

Reassigned Numbers Database 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).

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

INFORMATION ABOUT THE SYSTEM
Reassigned Numbers Database
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) The system may contain the RND registered users' contact information, payment information, and other technical information such as IP/MAC addresses.
IN WHAT SYSTEM OF RECORDS NOTICES (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? N/A
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? Sections 4(i)-(j), 201(b), 227, and 251(e) of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i)-(j), 201(b), 227, 251(e).
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:

☐ 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) AWS East West

- AWS API Gateway
- AWS CloudFront
- AWS Cognito
- AWS Dynamo DB
- AWS Elastic Beanstalk (not listed)
- AWS Lambda (not listed)
- AWS Relational Database Services
- AWS Secrets Manager
- AWS Simple Email Service
- AWS Simple Queue Service
- AWS Transfer (not listed)

☒ 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)

AWS East West

- AWS Route 53
- AWS S3
- Amazon EC2

[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 the they FedRAMP certified?**

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

Unless otherwise noted, the following AWS systems are in use and FedRAMP certified. Please note that AWS does not explicitly define its services as SaaS, PaaS, or IaaS, and as such the following classifications are based on the opinions of the assessor, according to the service's configuration.

Infrastructure-as-a-Service (IaaS)

Platform-as-a-Service (PaaS)

- AWS API Gateway
- AWS CloudFront
- AWS Cognito
- AWS Dynamo DB
- AWS Elastic Beanstalk
- AWS Lambda (not listed)
- AWS Relational Database Services
- AWS Secrets Manager
- AWS Simple Email Service
- AWS Simple Queue Service
- AWS Transfer (3PAO assessment in progress)
- Amazon EC2

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.

RND registered users' data will be collected for authorizing users to the system and to allow for the processing of subscription payments for access to the RND.

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 and a Letter of Authorization will be collected which will contain the following sets of data

- Agent
  - Name
  - Contact
  - Title
  - Phone Number
  - Company Email
- Caller
  - Company Name
  - Contact
  - Title
  - Telephone Number
  - Company Email

The Privacy Act Statement may be found here: https://www.reassigned.us/privacy

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

The scope of the information is being limited to that in the Technical Requirement document.

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

The SomosGov subscription process includes a validation step to have the subscriber validate that provided information is accurate, complete and up-to-date.

[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?

N/A – third-party systems are not documented in CSAM

There are no Information Sharing Agreements (ISA) in place.

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")?

Related billing information may be shared with the payment processor through an automatic API interface; users have the option to store their payment information with the payment processor for subscription renewal purposes.

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

Records in the systems in this boundary will be retained and disposed of consistent with the Federal Records Act and any applicable records schedule approved by the National Archives and Records Administration (NARA). Until NARA has approved a records schedule, SomosGov will maintain records in the system of records in accordance with NARA records management directives.

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**

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

SomosGov protects its information resources with a dynamic set of security measures leveraging system specific and Somos corporate controls. Some of these measures (e.g., network firewalls, physical security) protect SomosGov, while other measures (e.g., user

access restrictions, encryption) are applied to specific information systems, like those in the RND Boundary. Following the risk-based policy established in the Federal Information Modernization Act (FISMA), SomosGov applies more security measures (also known as security "controls") to information systems that present higher operational risks. Consistent with this policy, SomosGov applies specific security controls to systems that collect and process PII. A comprehensive list of the security and privacy controls SomosGov may apply to its information systems can be found in National Institute of Standards and Technology (NIST) Special Publication No. 800-53 (current version), https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/800-53.

SomosGov relies on two external providers to process user payments for subscription access to the RND: Chargbee acts as the gateway between the RND and Authorize.net which processes the user's payment. Both Chargebee and Authorize.net are certified as following the Data Security Standards (DSS) set by the Payment Card Industry (PCI) Security Standards Council to protect payment account data throughout the payment lifecycle and include standards on security practices technologies and processes, and standards for developers and vendors for creating secure payment products and solutions. PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices, https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

SomosGov relies on Google reCAPTCHA to protect the RND website by detecting abusive, non-user interactive traffic. reCAPTCHA sets a necessary cookie for the purpose of providing risk analysis. It may collect information with respect to the user interaction with the site, including date, time and length of the view, typing patterns (to detect nonhuman interaction), mouse clicks and screen touches, and answers to questions to verify that the user is not a robot.

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.

The system does not inherit privacy controls from AWS, Google reCAPTCHA, Chargebee, and Authorize.net. Google reCAPTCHA requires the RNDA to explicitly inform visitors to the site that reCAPTCHA is being used and to provide its users with a privacy policy.

1.6. Access to the Information

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

FCC employees from the Consumer and Governmental Affairs Bureau (CGB) and Enforcement Bureau will have read only access to the PII. This specifically refers to an employee of the FCC or an individual authorized by the FCC who uses the System to view information on Disconnected Telephone Numbers (TNs), Service Provider data submissions, and Caller queries via reports and queries. For the FCC, there will be a "Primary Contact" from CGB who will have account administration capabilities in the system such as giving access to others at the FCC who will have read only access to information on data submission and Caller queries, including the ability to query TNs and run reports.

Access to the systems within the RND Boundary is restricted to authorized FCC staff, as well as SomosGov and Somos system owners and end users. All system owners and end users must adhere to the SomosGov and applicable Somos policies and ensure that access to any PII stored in the RND system is appropriately limited. Access to the information stored within the RND System 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.

SomosGov staff must also follow the reporting and other procedures in the FCC's Breach Notification Policy.

B. Does this system leverage Enterprise Access Controls?

Yes.

C. Does the system leverage the FCC's Accounting for Disclosure control?

N/A – the RND is not a system of records as that term is defined by the Privacy Act.