Federal Communications Commission
Washington, D.C. 20554

January 13, 2022

Corina Henriques, Senior Director
SomosGov, Inc.
North American Numbering Plan Administrator and
Reassigned Numbers Database Administrator
Two Tower Center Boulevard
20th Floor
East Brunswick, New Jersey 08816-1100

Re: Executive Order on Improving the Nation's Cybersecurity

Dear Ms. Henriques:

This letter addresses the Executive Order on *Improving the Nation's Cybersecurity* issued on May 12, 2021.[1] The Executive Order establishes specific measures to: (1) improve the nation's cybersecurity and protect federal networks, including information sharing between the U.S. government and the private sector; (2) modernize and implement stronger cybersecurity standards in the Federal government and improve software supply chain security; (3) establish a cybersecurity safety review board; (4) create a standard playbook for responding to cyber incidents; and (5) improve detection of cybersecurity incidents on Federal government networks, including investigative and remediation capabilities. In accordance with the Executive Order, the Federal Communications Commission (FCC) must assess the protection of its federal networks used in partnership with third-party service providers. We also recognize that the Federal Acquisition Regulation Council has yet to adopt new provisions and contract clauses applicable to third-party service providers as outlined in the Executive Order.[2] We therefore direct SomosGov, Inc. (SomosGov), a third-party service provider of the FCC that conducts an array of day-to-day functions on behalf of the FCC, to start taking the necessary steps outlined within this letter to ensure appropriate cybersecurity requirements within your information technology (IT) enterprise.[3]

The Executive Order specifically seeks to ensure that IT, operational technology (OT), and information and communications technology (ICT) service providers can promptly notify a contracting agency of cyber threat and incident information on Federal Information Systems as well as cyber-incidents involving a software product or service.[4] To ensure further compliance with the FCC Cyber Security Program,[5] including the Federal Information Security Management Act (FISMA),[6] and the Executive Order, we direct SomosGov to implement the following:

[1] Improving the Nation's Cybersecurity, Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021) (Exec. Order No. 14028).

[2] Exec. Order No. 14028, Sect. 2(b)-(l).

[3] Exec. Order No. 14028, Sect. 2(a).

[4] Exec. Order No. 14028, Sect. 2(a)-(l).

[5] FCC Cyber Security Program, FCCINST 1479.5, https://www.fcc.gov/sites/default/files/fcc-directive-1479.5.pdf.

[6] 44 U.S.C. § 3541.

- **Cyber Incident Reports**. SomosGov shall evaluate its processes for collecting and preserving data, and responding to a cyber incident, including the steps it takes to identify and mitigate a threat and sharing that data with the FCC.
- **Multifactor Authentication (MFA)**. SomosGov shall review the National Institute of Standards and Technology (NIST)'s Digital Identity Guidelines, SP 800-63-3, to determine the appropriate level of authentication required for its IT enterprise.
- **Encryption at Rest and In-transit**. SomosGov shall determine the appropriate level of encryption required for its IT enterprise using the following NIST guides:
    - SP 800-209, Security Guidelines for Storage Infrastructure
    - SP 800-175A, Guide for Using Crypto Standards: Directives, Mandates, Policies
    - SP 800-175B Rev. 1, Guide for Using Crypto Standards: Cryptographic Mechanisms
    - SP 800-67 Rev. 2, Recommendation for the TDEA Block Cipher

We also highly encourage SomosGov to consider implementing the following steps to modernize its approach to cybersecurity:

- Implement a zero trust architecture framework for its internal and external information systems.[7]
- Develop a Cyber Supply Chain Risk Management (C-SCRM) program that identifies, assesses, and mitigates cyber supply chain risks at all levels.[8]
- Enhance management and use of audit logging in accordance with OMB M-21-31.

Lastly, we direct SomosGov, by no later than one year from the date of this letter, to comply with the terms of this letter. In the interim, SomosGov shall provide monthly progress reports during its recurring meetings with FCC IT.

Thank you for your prompt attention and commitment to these matters, and please address any questions or concerns to FCC IT program manager, Mr. Jasson Soemo, at (202) 418-1614, or Jasson.Soemo@fcc.gov.

Sincerely,

Mark Stephens
Digitally signed by Mark Stephens
Date: 2022.01.13 17:05:42 -05'00'

Mark Stephens
Managing Director

Kris A. Monteith
Chief, Wireline Competition Bureau

Patrick Webre
Chief, Consumer and Governmental Affairs Bureau

[7] *See* NIST, SP 800-207, *Zero Trust Architecture*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[8] *See* Cyber Supply Chain Risk Management, Overview, https://csrc.nist.gov/projects/cyber-supply-chain-risk-management. As of October 28, 2021, NIST released its second draft, Special Publication (SP) 800-161 Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft2.pdf.