4.5.2 Develop a Strategy to Secure Foundational Internet Protocols and Email

This proposal requires the National Telecommunications and Information Administration and the Department of Homeland Security to develop a strategy and recommendations, in consultation with internet service providers and civil society and academic experts, to define common, implementable guidance for securing the public core of the internet, including the Domain Name System and Border Gateway Protocol.

A BILL

To develop a strategy to secure the public core of the internet.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. 1. SECURE FOUNDATIONAL INTERNET PROTOCOLS.

(a) Definitions.—In this section:

(1) BORDER GATEWAY PROTOCOL.—The term "border gateway protocol" means a protocol designed to optimize routing of information exchanged through the internet.

(2) DOMAIN NAME SYSTEM.—The term "domain name system" means a system that stores information associated with domain names in a distributed database on networks.

(3) INFORMATION AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE PROVIDERS.—The term "information and communications technology infrastructure providers" means all systems that enable connectivity and operability of internet service, backbone, cloud, web hosting, content delivery, domain name system, and software-defined networks and other systems and services.

(b) Creation of a Strategy to Secure Foundational Internet Protocols.—

(1) PROTOCOL SECURITY STRATEGY.—In order to secure foundational internet protocols, not later than December 31, 2021, the National Telecommunications and Information Administration and the Department of Homeland Security shall submit to Congress a strategy to secure the border gateway protocol and the domain name system.

(2) STRATEGY REQUIREMENTS.—The strategy required under paragraph (1) shall—

(A) articulate the motivation and goal of the strategy to reduce incidents of border gateway protocol hijacking and domain name system hijacking;

(B) articulate the security and privacy benefits of implementing security for the border gateway protocol and the domain name system and the burdens of implementation and the entities on whom those burdens will most likely fall;

(C) identify key United States and international stakeholders;

(D) outline varying security measures that could be used to secure or provide authentication for the border gateway protocol and the domain name system;

(E) identify any barriers to implementing security for the border gateway protocol and the domain name system at scale;

(F) propose a strategy to implement identified security measures at scale, accounting for barriers to implementation and balancing benefits and burdens, where feasible; and

(G) provide an initial estimate of the total cost to the Government and implementing entities in the private sector of implementing security for the border gateway protocol and the domain name system and propose recommendations for defraying these costs, if applicable.

(3) CONSULTATION.—In developing the strategy required under paragraph (1) the National Telecommunications and Information Administration and the Department of Homeland Security shall consult with information and communications technology infrastructure providers, civil society organizations, relevant nonprofit organizations, and academic experts.