May 16, 2024

# FCC FACT SHEET[*]

## Reporting on Border Gateway Protocol Risk Mitigation Progress

Notice of Proposed Rulemaking PS Docket Nos. 24-146 and 22-90

### Background:

The Internet consists of tens of thousands of interconnected, independently administered networks. The Border Gateway Protocol (BGP) is the global inter-domain routing protocol used to exchange reachability information amongst these networks in order to route traffic across the Internet.

BGP's initial design, which remains widely deployed today, did not include security features to ensure trust in the information that is relied upon to route Internet traffic. As a result, a malicious actor or adversary can exploit BGP's vulnerabilities and deliberately falsify reachability information to redirect Internet traffic. Such exploits can expose Americans' personally identifiable information, enable theft, extortion, and state-level espionage, and can disrupt services upon which the public or critical infrastructural sectors rely.

In view of these vulnerabilities, service providers must take steps to secure Internet traffic originating from, or destined to, their networks. Although there have been multiple efforts by a variety of stakeholders over the past twenty years to address BGP security issues, more needs to be done. Since the Commission has authority to protect national security, as well as address practices that are unjust, unreasonable, or unreasonably discriminatory, the Commission needs to play an essential role in securing Internet routing.

### What the NPRM Does:

- The NPRM seeks to increase the security of the information routed across the Internet by proposing certain obligations on providers of broadband Internet access services (service providers) and their use of Border Gateway Protocol (BGP) and the Resource Public Key Infrastructure (RPKI). The RPKI helps to create trust in reachability information by enabling cryptographically verifiable associations between specific IP address blocks, or autonomous system numbers (ASNs), and the "holders" of those Internet number resources.
- Service providers would be required to prepare and maintain confidential BGP Routing Security Risk Management Plans (BGP Plans) that describe and attest to the specific efforts they have made, and further plans they intend to undertake, to create and maintain Route Origin Authorizations (ROAs) in the RPKI. The BGP Plans, which could be risk-based performance plans, would also have to attest to the extent to which the service provider conducts Route Origin Validation (ROV) filtering at interconnection points with peers and clients. The Plans would also provide goals and timetables for RPKI implementation. Nine large service providers would be required to file initial BGP Plans and resubmit updated versions annually thereafter. Subsequent BGP Plans would not need to be filed by large providers that attest that they are maintaining ROAs covering at least 90% of originated routes for IP address prefixes under their control.
- Additionally, the nine service providers would be required to file specific data quarterly in order to measure progress in ROA registrations and assess the reasonableness of the service provider's BGP Plan.
- Last, the NPRM seeks comment certain other measures related to implementing RPKI-based security.

[*] This document has been circulated for tentative consideration by the Commission at its June open meeting. The issues referenced in this document and the Commission's ultimate resolution of those issues remain under consideration and subject to change. This document does not constitute any official action by the Commission. However, the Chairwoman has determined that, in the interest of promoting the public's ability to understand the nature and scope of issues under consideration, the public interest would be served by making this document publicly available. The FCC's *ex parte* rules apply and presentations are subject to "exempt" *ex parte* rules. *See*, e.g., 47 C.F.R. §§ 1.1204, 1.1200(a). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR §§ 1.1200(a), 1.1203.

**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Reporting on Border Gateway Protocol Risk Mitigation Progress | ) | PS Docket No. 24-146 |
| | ) | |
| Secure Internet Routing | ) | PS Docket No. 22-90 |

# NOTICE OF PROPOSED RULEMAKING[*]

**Adopted: [ ]** **Released: [ ]**

**Comment Date: (30 days after date of publication in the Federal Register)**
**Reply Comment Date: (45 days after date of publication in the Federal Register)**

By the Commission:

## TABLE OF CONTENTS

Heading Paragraph #

[*] This document has been circulated for tentative consideration by the Commission at its June 2024 open meeting. The issues referenced in this document and the Commission's ultimate resolution of those issues remain under consideration and subject to change. This document does not constitute any official action by the Commission. However, the Chairwoman has determined that, in the interest of promoting the public's ability to understand the nature and scope of issues under consideration, the public interest would be served by making this document publicly available. The FCC's ex parte rules apply and presentations are subject to "exempt" ex parte rules. See, e.g., 47 C.F.R. §§ 1.1204, 1.1200(a). Participants in this proceeding should familiarize themselves with the Commission's ex parte rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. See 47 CFR §§ 1.1200(a), 1.1203.

## I. INTRODUCTION

1. The Internet is inextricably interwoven into the fabric of modern life, facilitating our daily activities, from work, education, and healthcare, to commerce, community, communication, and free expression.[1] Disruptions of communications can easily have significant cascading effects on other critical infrastructure sectors that rely on communications.[2]

2. Today, we take important next steps in addressing vulnerabilities threatening the security and integrity of the Border Gateway Protocol (BGP), which is central to the Internet's global routing system. BGP is the routing protocol used to exchange reachability information amongst independently managed networks on the Internet. BGP's initial design, which remains widely deployed today, did not include security features to ensure trust in the information that it is used to exchange. Although there have been multiple efforts by a variety of stakeholders over the past twenty years to address BGP security issues, more needs to be done, and the Commission has an essential role in ensuring further concrete progress.

3. Specifically, in this *Notice of Proposed Rulemaking* (*Notice*) we propose a number of steps applicable to providers of broadband Internet access service (BIAS) (service providers) designed to

[1] *Safeguarding and Securing the Open Internet*, WC Docket No. 23-320, Declaratory Ruling, Order, Report and Order, and Order on Reconsideration, paras. 1, 26 (2024)(*2024 Open Internet Order*).

[2] U.S. Government Accountability Office, Critical Infrastructure Protection: CISA [the Cybersecurity and Infrastructure Security Agency] Should Assess the Effectiveness of its Actions to Support the Communications Sector at 1 (2021), https://www.gao.gov/assets/d22104462.pdf [https://perma.cc/F5VK-GA8Q] (explaining how the Communications sector is integral to the U.S. economy and vital to national security since it underlies the operations of businesses, public safety organizations, and government).

improve the security of BGP routing.[3] Specifically, we are proposing that all such providers prepare and update confidential Border Gateway Protocol security risk management plans (BGP Plans or Plans) at least once a year. A BGP Plan would describe and attest to the specific efforts the service provider has made, and plans to undertake, to secure its BGP routing architecture using Resource Public Key Infrastructure (RPKI) as well as other methods at its disposal (e.g., peer-locking). The BGP Plans would include, among other things, a service provider's plans for Route Origin Authorization (ROA) registration and maintenance for its route originations and the status of and plans for its deployment of Route Origin Validation (ROV).[4] We propose to require a select number of the largest, most significant service providers to file their BGP Plans with the Commission, with the plans of the remaining service providers available to Commission staff upon request. In addition to the BGP Plan proposals, we propose quarterly reporting of selected data by service providers that would help us measure progress in RPKI deployment and assess whether additional measures may be needed. Finally, we seek comment on proposals to address cases where the service providers are not in a position today to take the foundational step of registering ROAs for the implementation of RPKI.

4. These proposals are part of ongoing multi-stakeholder efforts to address secure Internet routing issues. The National Cybersecurity Strategy, for instance, highlights the critical nature of securing the technical foundation of the Internet and expressly identifies addressing BGP vulnerabilities as among the most urgent of pervasive concerns today.[5] To further that objective, Initiative 4.1.5 of the National Cybersecurity Strategy Implementation Plan tasks the Office of the National Cyber Director (ONCD), working with key stakeholders and other Federal Government entities, to develop a roadmap to increase adoption of secure Internet routing techniques, including those that address BGP security concerns.[6] In addition, this *Notice* recognizes the importance of increased outreach and education about the security risks inherent to BGP, and of the role that the American Registry for Internet Numbers (ARIN), the U.S.-based Regional Internet Registry (RIR)[7] and its processes play in the deployment of RPKI-enabled improvements to BGP security, and seeks comment on possible additional steps that can be taken to facilitate deployment of RPKI-based routing security.

## II. BACKGROUND

5. In our Secure Internet Routing Notice of Inquiry (*Secure Internet Routing NOI*), the Commission outlined how various services that the public relies on are enabled by the Internet.[8] More recently, the Commission further emphasized the importance of the Internet, explaining that the Internet

[3] *2024 Open Internet Order* at paras. 28, 125-26. We also seek comment on whether there are additional service providers that use BGP to route Internet traffic that should be included within the scope of that definition.

[4] Réseaux IP Européens (RIPE) Network Coordination Centre, *Managing ROAs*, https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/resource-certification-roa-management/ [https://perma.cc/9ED5-ARFX] (last visited Apr. 29, 2024) (delineating the three informational elements contained in a ROA and describing it as "a cryptographically signed object that states which Autonomous System (AS) is authorised to originate a certain prefix.").

[5] Executive Office of the President, National Cybersecurity Strategy at 23-24 (2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/QQV7-XCGB] (*Biden NCS*).

[6] Executive Office of the President, National Cybersecurity Strategy Implementation Plan at 38 (2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf [https://perma.cc/CR9D-6KHK] (*Biden NCSIP*)(describing the title of Initiative 4.1.5 as "Collaborate with key stakeholders to drive secure Internet routing").

[7] Number Resource Organization (NRO), *Regional Internet Registries* (Feb. 27, 2024), https://www.nro.net/about/rirs/ [https://perma.cc/XP2H-BRQ5].

[8] *Secure Internet Routing*, PS Docket No. 22-90, Notice of Inquiry, 37 FCC Rcd 3471, 3471-72 para. 1 (2022)(*Secure Internet Routing NOI*).

serves as a platform for competition, free expression, and innovation, while also driving economic growth.[9] As was underscored during the COVID-19 Pandemic, though the trend had been clear before, the Internet is integral to our daily activities, from work, education, and healthcare, to commerce, community, communication, and free expression.[10] The Internet therefore now constitutes a key part of the national cyber infrastructure, enabling connectivity for use by both the public as well as operators of critical infrastructural services, including banking, the electrical power grid, fuel pipelines, and water processing plants.[11] Internet use has become even more prevalent since the COVID-19 Pandemic. In a Pew Research poll, 58% of participating adults described Internet access as essential.[12]

6. The Internet consists of "tens of thousands" of interconnected, independently administered and managed constituent networks.[13] Each such independently administered network is termed an Autonomous System (AS)[14] and achieves and maintains interconnection by using the Internet's sole global inter-domain routing protocol, the Border Gateway Protocol (BGP). As highlighted in the *Secure Internet Routing NOI*, BGP is a central component of the Internet, allowing the exchange of reachability information amongst the independently managed constituent networks.[15] BGP is so vital to the Internet that it has been referred to as "the 'glue' that enables the modern Internet."[16]

7. Despite being essential to the Internet, BGP does not have adequate built-in security measures, as its operational debut about 30 years ago featured mostly academic and research organizations. The contingency that significant threat vectors might become prevalent in Internet contexts was not widely anticipated at the time. As noted by federal agencies commenting in response to the *Secure Internet Routing NOI*, when the key portions of the design of BGP were finalized about three decades ago the need for such security was not anticipated.[17] The Internet today is very different, "due to the subsequent increase in the Internet's complexity and scale, with the rise of cybercrime, government cyber-conflict and other threats."[18]

8. Because the Internet has taken on an increasingly central role in everyday life, the vulnerabilities posed by this shortfall have begun to pose tremendous infrastructural risks. Many of the independently administered ASes interconnected by BGP are essential to the daily functioning of our

[9] *2024 Open Internet Order* at paras. 1, 26.

[10] *Id*.

[11] Department of Homeland Security, A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level at 43 (2008), https://www.dhs.gov/xlibrary/assets/nipp_srtltt_guide.pdf [https://perma.cc/8CD8-D4RV].

[12] Pew Research Center, *The Internet and the Pandemic* (Sept. 1, 2021), https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/ [https://perma.cc/JB78-TH4J].

[13] Broadband Internet Technical Advisory Group (BITAG), Security of the Internet's Routing Infrastructure at 6 (2022), https://www.bitag.org/documents/BITAG_Routing_Security.pdf [https://perma.cc/PPD6-WD6L] (*BITAG Report*).

[14] Cloudflare, *What is an autonomous system?*, https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/ (last visited Apr. 3, 2024)(*What is an autonomous system?*); *BITAG Report* at 6.

[15] *Secure Internet Routing NOI*, 37 FCC Rcd at 3471-72, para. 2.

[16] National Institute of Standards and Technology (NIST), *Technical Details*, (Mar. 9, 2023), https://www.nist.gov/programs-projects/robust-inter-domain-routing/technical-details [https://perma.cc/67KQ-FR74].

[17] CISA Comments at 1 (explaining how the original infrastructure of the Internet was built on mutual trust); *see* U.S. Department of Justice and U.S. Department of Defense (DOJ/DOD) Comments at 2 (explaining how "BGP was not designed to include security measures.").

[18] *BITAG Report* at 3.

critical infrastructure.[19] Due to the Internet's pervasiveness, the security of BGP is not only critical to public safety but is also critical to national security.[20]

9. BGP vulnerabilities can lead to actors in the distributed routing system of the Internet either intentionally or accidentally disrupting the flow of Internet traffic. This can cause interruption or cessation of access to services that the public or critical infrastructural sectors rely on, and/or misdirect communications and allow interception and blackholing, inspection, or manipulation of data.[21] Vulnerabilities in BGP allow for routing incidents to occur, which can impact both large sections of the Internet routing system, as well as the networks BGP connects.[22] Such routing security incidents can have serious implications for the traffic transiting networks.[23] As noted in the *Secure Internet Routing NOI*, some of the more commonplace incidents include BGP "hijacks."[24]

10. Numerous examples exist that highlight how routing incidents affect communications. Facebook's five-hour global outage in October 2021 was caused in part by a failure of its BGP routing which removed routes to its authoritative Domain Name System servers and resulted in more than 1.2 trillion person-minutes of service unavailability. [25] To its users, it was as if Facebook, and its other services such as Messenger and Instagram, disappeared from the Internet. Another example occurred in 2019, when an Internet Service Provider (ISP) in Pennsylvania—DQE Communications—started to announce routes for Cloudflare, Amazon, and Linode because of a technical error by one of its network administrators.[26] This error caused destinations served by these networks to become unreachable from some parts of the Internet. As another example, in 2020 there was a BGP hijack by a network ostensibly controlled by Rostelecom, which prompted significant service disruptions to entities across the globe. According to the analysis from the Mutually Agreed Norms for Routing Security (MANRS), the incident could have been prevented if Rascom—a directly connected peer to Rostelecom—had implemented strict RPKI ROV filtering to ensure misoriginated routes did not propagate.[27] This incident began when Rostelecom misoriginated routes to several CDNs. Rascom, if it were using RPKI ROV, could have rejected these routes and not propagated them, thus curtailing the attack. An additional incident was reported in an article from 2018, after China Telecom had misdirected U.S. Internet traffic—for two and a

[19] *BGP NOI*, 17 FCC Rcd at 3471, para. 5.

[20] CISA Comments at 1.

[21] *BITAG Report* at 8-9.

[22] Organisation for Economic Cooperation and Development (OECD), Routing Security: BGP Incidents, Mitigation Techniques and Policy Actions at 3 (2022), https://www.oecd-ilibrary.org/docserver/40be69c8-en.pdf?expires=1710269922&id=id&accname=guest&checksum=7ED2936E74CB5A7B046B3EC2EFE8035F [https://perma.cc/Q3HU-89JW] (*OECD Report*).

[23] *OECD Report* at 11.

[24] *Secure Internet Routing NOI*, 37 FCC Rcd at 3471-72, para. 2; *Id.* at 3473, para. 5 ("Causing Internet traffic to depart from its most efficient path is termed 'BGP hijacking.'"); *see also BITAG Report* at 38; *OECD Report* at 11 (A BGP hijack occurs when a network announces reachability to an IP prefix, or multiple IP prefixes, which is invalid (i.e., to which the network does not have a valid route (or "reachability"))).

[25] Akamai, *What Is Authoritative DNS?*, https://www.akamai.com/glossary/what-is-authoritative-dns [https://perma.cc/8GGT-3TLF] (last visited May 1, 2024); *OECD Report* at 3.

[26] Kieren McCarthy, *BGP super-blunder: How Verizon today sparked a 'cascading catastrophic failure' that knackered Cloudflare, Amazon, etc* (June 24, 2019), https://www.theregister.com/2019/06/24/verizon_bgp_misconfiguration_cloudflare/ [https://perma.cc/KE4C-2FBG].

[27] Aftab Siddiqui, *Not just another BGP Hijack* (Apr. 6, 2020), https://manrs.org/2020/04/not-just-another-bgp-hijack/ [https://perma.cc/LGH6-PWW7]. *See* Hurricane Electric, *BGP Toolkit*, https://bgp.he.net/AS20764 [https://perma.cc/63UH-Z3A9] (last visited May 14, 2024)(showing connected peers for an autonomous system number belonging to Rascom).

half years—to one of China Telecom's networks.[28] This misdirection of U.S. routes occurred because an autonomous system on the China Telecom backbone "incorrectly handled routing announcements for AS703, an [AS] belonging to Verizon."[29] Although it is unknown whether the misdirection occurred deliberately or accidentally, it is the vulnerabilities inherent in BGP that allowed for the misdirection to happen.[30]

11. There have also been clear, deliberately caused routing incidents. In one example an adversary employed a BGP hijack against a cryptocurrency service to effect theft.[31] In another incident, Russian network operators are suspected of having exploited BGP's vulnerability to redirect a BGP routing incident, disrupting financial services on the eve of Russia's invasion of Ukraine in February 2022.[32] In 2020, a Russian digital services provider diverted Internet traffic from Google, Facebook, Akamai, Cloudflare, and Amazon through Russia that resulted in the routed data not reaching the intended recipient.[33] The threat of Internet traffic disruption, interception, and blackholing due to deliberate adversarial manipulation of BGP is undeniable.

12. For all these reasons, finding and implementing remedies to the vulnerabilities in BGP continues to grow more pressing. Ensuring that adequate countermeasures are implemented to offset BGP vulnerabilities has become a pressing matter for the U.S. Government. Other agencies of the Federal Government have recognized the need for the Federal Communications Commission (FCC or the Commission), as the telecommunications regulator, to play a critical role in this context.[34]

### A. Border Gateway Protocol and the Development of RPKI-Based Origin Validation

13. Networks interconnected by BGP, termed BGP Autonomous Systems (ASs), are referred to by the Autonomous System Numbers (ASNs)[35] assigned by the Regional Internet Registry (RIR) that oversees Internet number resource allocation and related coordination in that network's geographical area.[36] An AS may include one or multiple separate networks, collectively all under the technical administration of a single entity. For BGP purposes, a network path is denoted as a string of ASNs termed an AS Path. The AS Path is one of the "BGP path attributes" or control variables used in

[28] Eric Preizkalns, *China Telecom Misdirected US Net Traffic Through China* (Nov. 12, 2018), https://commsrisk.com/china-telecom-misdirected-net-traffic-through-china/ [https://perma.cc/98NY-A3P9].

[29] *Id.*

[30] *Id.*

[31] NIST, NIST SP 800-30, Guide for Conducting Risk Assessments at B-1 (2012), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (defines an adversary as an "[i]ndividual, group, organization, or government that conducts or has the intent to conduct detrimental activities); Doug Madory, *What can be learned from recent BGP hijacks targeting cryptocurrency services?* (Sept. 22, 2022), https://www.kentik.com/blog/bgp-hijacks-targeting-cryptocurrency-services/.

[32] The term "network operator" can refer to enterprise networks or service providers. *See* Matthew Wilder, *The Business Case for IPv6: Internet vs. Intranets* (Feb. 6, 2023), https://www.arin.net/blog/2023/02/06/ipv6-lets-grow-business-case-pt1/ [https://perma.cc/UD9E-YGQF] (explaining how network operators that are service providers, such as ISPs, may take different steps to deploy IPv6, compared to other types of network operators, such as enterprise networks).

[33] Angelique Medina, *Why Rostelecom's Route Hijack Highlights the Need for BGP Security* (Apr. 2, 2020), https://www.thousandeyes.com/blog/rostelecom-route-hijack-highlights-bgp-security [https://perma.cc/3B9H-3387].

[34] DOJ/DOD Comments at 1; CISA Comments at 1.

[35] Each of the interconnected constituent networks that comprise the Internet are referred to as an Autonomous System (AS) and are uniquely identified by a numeric Autonomous System Number (ASN). *BITAG Report* at 6.

[36] Number Resource Organization (NRO), *Regional Internet Registries* (Feb. 27, 2024) https://www.nro.net/about/rirs/ [https://perma.cc/XP2H-BRQ5]; *What is an autonomous system?.*

signaling destination reachability that influences how each BGP speaker selects routes to that specific destination. For more information, please refer to Appendix A, which provides additional background on inter-domain routing.[37] As designed, BGP provides no intrinsic means by which to verify either the originator of a route or the rest of the AS Path in that route, either of which can be manipulated for use as attack vectors instrumental in BGP hijacks.[38] This lack of origin and path validation creates routing vulnerabilities, posing threats to public safety and security by potentially exposing U.S. citizens' personally identifiable information and enabling theft, extortion, and state-level espionage, in addition to disrupting potentially critical communications.[39] Network operators must take steps to counter these threats to secure traffic originating from, or destined to, their networks. However, the pervasiveness of the Internet, together with the autonomous administration of its many constituent networks, constrains the solutions possible to address these issues.[40]

14. To improve the degree to which communications infrastructures can be protected from the vulnerabilities discussed above, both origin validation and path validation are necessary. We focus in this *Notice* on techniques for origin validation, and particularly on RPKI-based origin validation, standardization of which began more than ten years ago.

15. Origin validation consists of verifying that a network is authorized to originate a route advertisement containing a specific Internet protocol (IP) prefix and is a necessary step to securing Internet routing.[41] A previous attempt to verify the veracity of route originations resulted in the Internet Route Registry system, which although it has been in use since 1995, is known to have substantial inaccuracies.[42] A much more effective approach for securing origin integrity is enabled by the RPKI, which originated in papers dating from 2000. The RPKI includes cryptographic attestations that facilitate higher trust in route origination and other routing information and was standardized in 2012.[43]

[37] Deep Medhi & Karthik Ramasamy, Network Routing: Algorithms, Protocols, and Architectures (2d ed. 2017) (provides further background information on inter-domain routing).

[38] T. Manderson, K. Sriram & R. White, Use Cases and Interpretations of Resource Public Key Infrastructure (RPKI) Objects for Issuers and Relying Parties (2013), https://www.rfc-editor.org/info/rfc6907 [https://perma.cc/3JUZ-D8M3].

[39] NIST, NIST SP 1800-14, Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation at 6 (2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-14.pdf.

[40] It would be difficult, if not impossible to alter the fundamentals of BGP protocol design. According to leading Internet technical experts, including staff from NIST, who participated in the SIDR Working Group of the Internet Engineering Task Force (IETF), and peers across industry, securing BGP operation and achieving resilient inter-domain connectivity must rely on a series of retrofits with no, or minimal changes to the protocol itself. *See* S. Murphy et al., *Retrofitting security into Internet infrastructure protocols*, 1 Proceedings DARPA Information Survivability Conference and Exposition, 3-17 (2000); *see also* P. Papadimitratos & Z. J. Haas, *Securing the Internet routing infrastructure*, 40 IEEE Communications Magazine 10, 60-68 (2002).

[41] An IP prefix is a contiguous set of IP addresses. *See* NIST, NIST Spec. Pub. 800-189, Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation, at 12-13 (2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189.pdf (*NIST SP 800-189*).

[42] Asia Pacific Network Regional Information Centre, *The Internet Routing Registry (IRR)*, https://www.apnic.net/manage-ip/apnic-services/routing-registry/ [https://perma.cc/W34H-KYG5] (last visited Apr. 26, 2024); Ben Du et al., IR Regularities in the Internet Routing Registry (Oct., 24, 2023), https://doi.org/10.1145/3618257.3624843 [https://perma.cc/YY2Z-5L6J].

[43] S. Kent, An Infrastructure Supporting Secure Internet Routing (2006), https://doi.org/10.1007/11774716_10; M. Lepinski & S. Kent, An Infrastructure to Support Secure Internet Routing (2012), https://www.rfc-editor.org/info/rfc6480 [https://perma.cc/9CE3-4CKH].

16. The RPKI enables cryptographically verifiable associations between specific IP address blocks or ASNs and the holders of those Internet number resources.[44] This enables the holders of Internet number resources to attest (via a chain of verifiable digital signatures) to which ASN should originate their IP address prefixes.[45] The Internet Assigned Numbers Association defines the "holder" of Internet number resources as an organization that has been allocated a block of IP addresses from their RIR.[46] For the purposes of this *Notice*, however, the "holder" of Internet number resources refers to an entity that: (1) is assigned IP address space by ARIN, or (2) has its own legacy address space, or (3) is a client of a service provider that has transferred IP prefixes to the client via contract.[47] In this last case, we understand that the holder of the address space has been changed from the provider to its client.

17. To take advantage of the routing security features enabled by the RPKI, entities participating in BGP routing need to register and maintain ROAs that correspond to the routes they originate, creating mappings between the associated IP prefixes and the originating ASNs. For a holder of IP address prefixes to authorize an ASN to originate a route to a set of IP prefixes it holds, it must first obtain a resource certificate from its issuing RIR that associates those IP prefixes with itself.[48] A resource holder will create signed ROAs after receiving a resource certificate from its RIR and generating the corresponding end-entity certificate.[49] Creating and maintaining accurate ROAs to authorize originated routes is the first step towards implementing origin validation using the RPKI.[50]

18. The other step necessary to implement RPKI-based origin validation is for an essential set of service providers to perform ROV filtering using the ROA repositories in order to validate the routes they accept.[51] Using ROV to validate the origin authenticity of a received route allows the service provider to filter routes found to be invalid.[52] The RPKI components, and the systems that utilize them, if

[44] *See* American Registry for Internet Numbers (ARIN), *Resource Certification (RPKI)*, https://www.arin.net/resources/manage/rpki/ [https://perma.cc/RDJ5-CK6Q] (last visited Apr. 15, 2024); RIPE NCC, *What is RPKI?*, https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/what-is-rpki/ [https://perma.cc/4RW9-8U3Z] (last visited Apr. 15, 2024)(*Resource Certification (RPKI)*).

[45] *Resource Certification (RPKI).*

[46] *See* Internet Assigned Numbers Authority (IANA), *Number Resources*, https://www.iana.org/numbers [https://perma.cc/T6YF-F764] (last visited Apr. 15, 2024); RIPE NCC, *RIPE NCC Services to Legacy Internet Resource Holders*, https://www.ripe.net/manage-ips-and-asns/legacy-resources/ripe-ncc-services-to-legacy-internet-resource-holders/ [https://perma.cc/2AE2-JZHK] (last visited Apr. 15, 2024).

[47] "Address space" colloquially refers to the collective IP addresses controlled by an ISP. *See, e.g.*, Leslie Noble, *ARIN Reaches Final /8 of IPv4 Address Space* (Apr. 24, 2014), https://www.arin.net/vault/blog/2014/04/24/arin-reaches-final-8-ipv4-address-space/ (describing the provision of "address space" by ARIN).

[48] *See Resource Certification (RPKI)*.

[49] M. Lepinski & S. Kent, RFC 6480 - An Infrastructure to Support Secure Internet Routing at 6-7 (2012), https://www.rfc-editor.org/info/rfc6480.

[50] *See OECD Report* at 24.

[51] Advanced Computing Systems Association (USENIX) Security Symposium, Tomas Hlavacek et al., *Keep Your Friends Close, but Your Routeservers Closer*: *Insights into RPKI Validation in the Internet*, 4841-58 (2023)("The burden of protecting the global routing architecture primarily lies on large service providers and Tier-1 providers. ROV implementation in Tier-1 providers greatly benefits Internet security as it limits the spread of hijacks to a localized scope."); Doug Madory & Job Snijders, Exploring the Latest RPKI ROV Adoption Numbers (May 24, 2023), https://www.kentik.com/blog/exploring-the-latest-rpki-rov-adoption-numbers/ ("If an AS doesn't reject RPKI-invalid routes, but its transit providers do, it is almost like they do, too. Unless, of course, the invalid routes are arriving over a peering connection, circumventing transit.").

[52] *See NIST 800-189* at 12-13.

implemented adhering to fundamental security practices, offer promising avenues to address BGP security vulnerabilities.[53]

19. The extent to which route originations are covered by ROAs, in addition to the accuracy of the ROAs themselves, determines the usefulness of ROV in subsequently filtering invalid routes, which in turn determines the effectiveness of RPKI-derived techniques as measures to improve routing security.[54] Sufficient coverage of originated routes with accurate and up-to-date ROAs is a prerequisite for network operators to realize the benefits from ROV filtering.[55] The subsequent filtering via ROV is critical to preventing BGP routing incidents, as demonstrated by the BGP hijack of an AS controlled by Rostelecom described above.

### B. FCC Efforts to Promote Secure Inter-Domain Routing

20. For more than a decade, the Commission has actively promoted improvements to the cybersecurity of networks, including those designed to counteract BGP vulnerabilities. For example, the Commission chartered Communications Security, Reliability, and Interoperability Councils (CSRICs)—federal advisory committees comprised of stakeholders from the telecommunications industry as well as special advisors from other relevant sectors—to address issues associated with the security of communications systems.[56] CSRICs III and VI, in particular, addressed issues and risks associated with BGP, which included recommendations and best common practice standards to mitigate these risks.[57]

21. The CSRIC III working group active in the 2011-2013 period produced a report which outlined then-current best practices implemented by network operators, and recommended further actions to build on these.[58] This report recommended that network operators ensure that their Internet routing registry entries are accurate, complete, and up-to-date, and that network operators use the RPKI as a standards-based approach for providing cryptographically secure databases of Internet resources and routing authorizations.[59] The CSRIC III report made four recommendations related to RPKI-based origin validation: (1) maintain accurate records about number resource holders; (2) undergo cautious, staged deployment of RPKI origin validation; (3) undertake efforts to mitigate risks inherent in RPKI; and (4) suggestions for improving BGP security metrics and measurements.[60] As follow up to the CSRIC III report, the FCC sought comment on the implementation and effectiveness of the recommendations and

[53] Donika Mirdita et al., *The CURE To Vulnerabilities in RPKI Validation*, Network and Distributed System Security (NDSS) Symposium 2024 (2024).

[54] *See OECD Report* at 24.

[55] *Id.* at 24.

[56] Federal Communications Commission (FCC), *Communications Security, Reliability, and Interoperability Council*, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited Mar. 22, 2024).

[57] *See* Communications Security, Reliability, and Interoperability Council (CSRIC) III, Secure BGP Deployment, Final Report at 3 (2013), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_%202013.pdf (*CSRIC III Report*); *see also* CSRIC VI, Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols, Final Report at 3-7 (2019), https://www.fcc.gov/sites/default/files/csric6wg3_finalreport_030819.pdf (*CSRIC VI Report*).

[58] *CSRIC III Report* at 3.

[59] *Id.* at 4-5.

[60] *Id.* at 16-26.

alternatives that stakeholders have developed since the time of the CSRIC's original work to address those challenges.[61]

22. CSRIC VI built on the CSRIC III recommendations, and developed additional guidance suggesting that network operators support MANRS and Internet Engineering Task Force (IETF) Best Common Practice Standards.[62] MANRS recommendations identify four focus areas to improve routing security: (1) filtering to ensure accuracy of BGP route announcements; (2) anti-spoofing to enable source IP address validation for at least single-homed stub customer networks, their end users and supporting infrastructure; (3) coordination to ensure maintenance of accurate and current contact information in RIRs and associated databases (PeeringDB); and (4) global validation of routing information, which involves network operators publishing their data so others can validate it.[63] The CSRIC VI working group's final report more generally recommended further studies as new best practices are developed and industry implements existing security measures (e.g., RPKI).[64]

23. The FCC followed up in 2022 on the risks inherent to BGP, as well as countermeasures, with the release of the *Secure Internet Routing NOI*.[65] The *Secure Internet Routing* NOI sought comment on steps the Commission should consider taking to help protect and strengthen the nation's communications networks and other critical infrastructure from vulnerabilities intrinsic to BGP.[66] In particular, the *Secure Internet Routing* NOI sought comment on the security measures recommended by CSRIC III and VI (e.g., RPKI, MANRS, and applicable IETF Best Common Practice standards), and the extent to which network operators have implemented available BGP security recommendations developed by industry.[67]

24. A significant number of commenters on the *Secure Internet Routing NOI* strongly cautioned the Commission against implementing prescriptive measures regarding Internet routing security.[68] Some commenters agreed, however, that the Commission can still take "important steps" to promote routing security, such as working with our federal "government partners . . . to encourage a wider adoption of BGP tools and solutions that will enhance ecosystem security and address and mitigate vulnerabilities and potential exploits."[69] Some of those government agencies, while noting their own

[61] *FCC's Public Safety and Homeland Security Bureau Requests Comment on Implementation of CSRIC III Cybersecurity Best Practices*, Public Notice, 29 FCC Rcd 9217, 9217-18 (PSHSB 2014).

[62] *CSRIC VI Report* at 4-15, 6-20.

[63] *Id.* at 4-15 and 4-16.

[64] *Id.* at 20.

[65] *Secure Internet Routing NOI*, 37 FCC Rcd 3471.

[66] *Id.*

[67] *Id.*; *FCC's Public Safety and Homeland Security Bureau Requests Comment on Implementation of CSRIC III Cybersecurity Best Practices*, Public Notice, 29 FCC Rcd 9217 (2014).

[68] *See, e.g.,* Internet Society Reply at 2 ("While there are proactive actions the [USG] can take to improve routing security, like many other commenters we caution the Commission against prescriptive routing security mandates which could have serious unintended consequences."); Verizon Comments at 4 ("[T]he Commission should avoid imposing prescriptive approaches to routing security."); CTIA Comments at 29 ("Rather than promoting security, prescriptive mandates could lead to companies to focus on compliance and distract from the important work of developing consensus standards.").

[69] *See, e.g.,* NCTA Comments at 6 ("[W]hile the Commission should avoid taking a prescriptive approach to BGP, there are important steps that it could take to promote and enhance routing security. . . ."); Comcast Comments at 11 ("[T]he Commission should leverage its expert agency role to promote federal policies that encourage and facilitate the development and deployment of BGP security solutions more broadly."); USTelecom Comments at 10 ("[B]y leveraging its convening authorities to bring relevant voices to the table, the Commission can help the U.S.

(continued….)

roles in protecting national security in a variety of industry sectors, advocated for the Commission to take regulatory action to address the vulnerabilities that affect BGP.[70] For example, the Department of Defense (DOD) and the Department of Justice (DOJ) specifically commented that "existing routing security measures, like [RPKI], can help mitigate the risk[s]" inherent in BGP, and suggested that additional transparency measures may be appropriate and necessary, such as a "requirement to report peering and interconnection partners and to monitor and periodically audit traffic routing to ensure traffic is not being misrouted over untrusted networks."[71] DOD and DOJ further highlighted the national security concerns regarding BGP vulnerabilities, commenting that such vulnerabilities "put U.S.-person data and communications (including government communications) at risk of theft, espionage, and sabotage by foreign adversaries, both directly and through third parties."[72] Indeed, those agencies advocated "that the [Commission] should comprehensively tackle these [BGP] vulnerabilities with industry-wide solutions using a combination of technical security standards and transparency measures[.]"[73]

25. After the comment cycle on the *NOI* closed, the Commission changed the *ex parte* status of this proceeding from "permit-but-disclose" to "exempt" in order to "facilitate the free exchange of exploratory ideas among the staff of [f]ederal agencies and interested stakeholders working toward the important goal of promoting secure Internet routing."[74] This change allowed for more detailed FCC staff engagement with stakeholders to improve BGP security.[75] As part of these continuing efforts, in the summer of 2023, the FCC held a public workshop to further identify and discuss existing and potential safeguards to address BGP routing security issues.[76] At that public workshop, industry stakeholders and representatives from other U.S. Government agencies discussed the vulnerabilities inherent to BGP, actions taken to improve BGP security, and the potential for future actions to address the vulnerabilities.[77] Workshop participants emphasized the risk that adversaries—including state-level adversaries—pose, which may result in espionage, sabotage, or interference of communication networks in the United

[G]overnment, its allies and partners, and key private sector stakeholders to meaningfully advance BGP security and lay a working foundation for the many other cybersecurity challenges that lie ahead.").

[70] *See* DOJ/DOD Comments at 9-10; *id.* at 10 ("Consistent, technically informed, yet flexible rules provide the most effective framework for addressing security needs while providing the predictability required for private industry to make long-term investment decisions."); CISA Comments at 1 ("[B]ecause the BGP risk is systemic, no one entity or group of entities is responsible for its overall security. Similarly, no single entity reaps the benefits from unilaterally improving BGP security, making it difficult to organize private activities to solve the problem. Therefore, CISA recommends that the FCC investigate and consider methods to drive down this risk by utilizing all of its statutory authorities.").

[71] DOJ/DOD Comments at 5.

[72] *Id.* at 3.

[73] *Id.* at 1.

[74] *PSHSB Changes Ex Parte Status for Secure Internet Routing Proceeding*, PS Docket No. 22-90, Public Notice, 38 FCC Rcd 2506 (PSHSB 2023).

[75] *Id.*; *see* Letter from David Clark, Senior Research Scientist, Massachusetts Institute of Technology, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 22-90, at 1 (filed July 18, 2023); *see also* 47 CFR § 1.1200(a).

[76] *Public Safety and Homeland Security Bureau to Host Public Workshop on Border Gateway Protocol Security on July 31, 2023*, PS Docket No. 22-90, Public Notice (PSHSB 2023)(*BGP Workshop Public Notice*).

[77] *FCC Chairwoman Rosenworcel & CISA Director Easterly to Headline Border Gateway Protocol Security Workshop*, PS Docket No. 22-90, Advisory (PSHSB 2023); *see Border Gateway Protocol Security Workshop*, at 42:57 (July 31, 2023), https://www.fcc.gov/news-events/events/2023/07/bgp-security-workshop (*BGP Workshop*)(ONCD speaking about NSCIP Initiative 4.1.5); *BGP Workshop*, at 70:00 (AT&T speaking about its experience and process for addressing BGP vulnerabilities); *BGP Workshop*, at 76:00 (Verizon speaking about its experience and process for addressing BGP vulnerabilities).

States.[78] The RPKI and the avenues it affords to assist in better inter-domain routing security, including ROA and ROV were discussed as current tools available to reduce the risks posed by BGP vulnerabilities.[79] Industry stakeholders—both large and small—highlighted the efforts they have undertaken to incorporate these RPKI-facilitated measures into their routing security architectures.[80] The workshop examined the viability of emerging BGP security advancements such as Autonomous System Provider Authorizations (ASPA) to address path validation and other approaches to lessen the risks currently inherent in interdomain routing.[81]

26. The workshop provided industry leaders and the federal agencies a forum to share their expertise, concerns, and encourage the continued deployment of RPKI and ROAs. Participants of the workshop raised various concerns regarding the process of implementing RPKI-based routing security measures, including the operational challenges.[82] Notably, participants also highlighted an important issue regarding the customers of service providers to whom the service provider has transferred IP address prefixes. That is, in some cases a customer to whom IP address prefix(es) has been transferred from a service provider may be the only one that can register ROAs for that address space.

27. From these engagements, Commission staff gained valuable insight into the variety of approaches to, and the general industry progress in deploying routing security measures which make use of RPKI.[83] The insights gained from these engagements have substantially informed the proposals contained in this *Notice.* This continued engagement also has encouraged other routing security efforts by industry and by other federal agencies actively engaged on secure Internet routing issues, including CISA, DOJ, National Telecommunications and Information Administration (NTIA), and the National Institute of Standards and Technology (NIST).[84]

[78] *Chairwoman Rosenworcel Opening Remarks at Border Gateway Protocol Security Workshop*, PS Docket No. 22-90, Speech (PSHSB 2023); *see also* FCC, *The Most Important Part of the Internet You've Probably Never Heard Of* (Aug. 2, 2023), https://www.fcc.gov/news-events/notes/2023/08/02/most-important-part-internet-youve-probably-never-heard; *BGP Workshop*, at 08:35 (CISA Director Jen Easterly speaking about threats to national security due to BGP vulnerabilities).

[79] NIST, BGP Security Level Set Problem Spacing and Emerging Solutions at 8-9 (2023), https://www.fcc.gov/sites/default/files/NIST%20BGP%20Level%20Set-Problem%20Space-Emerging%20Solutions%20-%20FCC%20BGP%20Wrkshp073123.pdf (*NIST BGP Level Set*).

[80] Fredrik Korsbäck, How AWS is helping to secure internet routing at 3 (2023), https://www.fcc.gov/sites/default/files/AWS%20and%20Secure%20Internet%20Routing%20-%20FCC%20BGP%20Wrkshp073123.pdf; *see also* Anees Shaikh, BGP routing security: Cloud/Content providers at 3 (2023), https://www.fcc.gov/sites/default/files/Google%20CSP%20Routing%20Security%20-FCC%20BGP%20Wrkshp073123.pdf.

[81] *See NIST BGP Level Set* at 22.

[82] *See BGP Workshop*, at 86:11.

[83] *See* Andrew Gallo, *Community Takeaways From FCC Routing Security Workshop* (Sept. 21, 2023), https://internet2.edu/community-takeaways-from-fcc-routing-security-workshop/; *see also* CableLabs, Cybersecurity Framework Profile for Internet Routing at 5 (2024), https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2024/jan/cs2024_0014.pdf.

[84] *See* NIST, CSF 2.0 Implementation Examples at 23 (2024), https://www.nist.gov/system/files/documents/2024/02/21/CSF%202.0%20Implementation%20Examples.pdf (providing BGP monitoring as an example for the Continuous Monitoring (DE.CM) category); *see also* Memorandum from Majority Staff, House Committee on Energy and Commerce, to Members, Subcommittee on Communications and Technology at 6-7 (Jan. 9, 2024)(detailing how members of the Subcommittee on Communications and Technology were hearing testimony regarding cybersecurity issues including BGP on Jan. 11, 2024).

### C. Other Federal Efforts to Promote Secure Internet Routing

28. The Commission is working in concert with multiple other federal efforts that are addressing the vulnerabilities in BGP. Of greatest prominence today is Initiative 4.1.5, Secure Internet Routing, in the plan for implementing the President's National Cybersecurity Strategy. Initiative 4.1.5 in President Biden's National Cybersecurity Strategy Implementation Plan (NCSIP) tasks ONCD, which advises the President on cybersecurity policy and strategy, to collaborate with stakeholders and appropriate United States Government (USG) entities to create a roadmap for adopting "secure Internet routing techniques and technology."[85] The National Cybersecurity Strategy sets forth six encompassing pillars designed to create a safer and more resilient interconnected world, and explicitly addresses the need for securing the technical foundation of the Internet as part of that effort.[86] To meet this objective, the National Cybersecurity Strategy recommended exploring approaches and options to address BGP routing security concerns.[87] Namely, Initiative 4.1.5 in the NCSIP envisions five goals for its roadmap to increase the adoption of Internet routing techniques and technology: (i) identify security challenges; (ii) explore approaches to address concerns associated with Internet routing and BGP security; (iii) identify and inform the development of best practices; (iv) identify needed research and development; and (v) identify barriers to adoption and alternate mitigation approaches.[88] Contributing to the work on the Initiative are many other federal agencies, including NTIA, NIST, CISA, DOJ, the National Security Agency, and the Office of Science and Technology Policy.[89]

29. Securing the technical foundation of the Internet remains a key strategic objective in President Biden's National Cybersecurity Strategy, which specifically identifies the vulnerabilities in BGP as one of the "most urgent" and "pervasive concerns" needing to be addressed.[90] To address BGP's vulnerabilities and reach a more secure Internet ecosystem, the Strategy envisions "close collaboration between public and private sectors."[91] For example, the Strategy directs that: "The Federal Government will lead by ensuring that its networks have implemented these and other security measures while partnering with stakeholders to develop and drive adoption of solutions" as well as measures "to mitigate the most urgent of these pervasive concerns such as Border Gateway Protocol vulnerabilities."[92] It is the joint effort, between the USG and the holders of Internet number resources working independently, but also in concert with each other, that will help us reach a more secure Internet routing system.

30. NIST is one of the U.S. federal entities with which the FCC is working closely. The NIST Internet Technology Research Group, part of its Communications Technology Lab was funded by the US Federal Government to work on research and standardization efforts to improve the security of Internet routing and other infrastructural protocols such as Domain Name System Security Extensions. In 2019, NIST published Special Publication 800-189 (NIST SP 800-189), recommending the use of RPKI, BGP origin validation (BGP-OV), and prefix filtering for securing the interdomain routing control

[85] Executive Office of the President, National Cybersecurity Strategy Implementation Plan at 38 (2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf (*Biden NCSIP*).

[86] Executive Office of the President, National Cybersecurity Strategy at 1, 23-24 (Mar. 1, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (*Biden NCS*).

[87] *Id.* at 1, 23-24.

[88] *Biden NCSIP* at 38.

[89] *Id.* at 38.

[90] *Biden NCS* at 24.

[91] *Id.* at 24.

[92] *Id.* at 24.

traffic.[93] In particular, NIST SP 800-189 provided recommendations to ISPs associated with obtaining RPKI certificates, managing subordinate certificate authorities, registering ROAs in the global RPKI for announcement, and how to manage prefixes.[94] NIST SP 800-189 also provided recommendations for addressing various routing hijacks, such as securing against DoS attacks and reflection/amplification attacks, among others.[95]

31. NIST's Robust Inter-Domain Routing program works with industry, contributes in the IETF standardization process, and fosters the development and deployment of technologies to improve the security of BGP routing.[96] Further, the program includes the publicly accessible NIST RPKI Monitor tool, which measures the global deployment of RPKI.[97] The program also includes a list of accessible presentations, standards specifications, standards contributions, and panel sessions where NIST team members have participated.[98]

### D. Industry Efforts to Address Vulnerabilities

32. The FCC's interest in BGP security is shared with, and was preceded by, significant efforts in many quarters. Leading academics have been active in this sphere since the early part of this century.[99] Industry stakeholders, such as the Internet Society, an advocacy organization whose members are comprised of companies and non-profits, have emphasized the case for improving routing security and the essential nature of the RPKI to this effort.[100] The Internet Society launched and supports the initiative entitled MANRS, which is an industry-endorsed organization that is active in the effort to secure global routing, and whose set of best practices was recommended by CSRIC VI.[101] MANRS provides guidance for various entities that allow the Internet to function, including guidance on steps that network operators such as ISPs can take to secure routing.[102] These include taking measures, variously classified by ISOC/MANRS as "compulsory" or "recommended" to prevent propagation of incorrect routing information, facilitating global operational communication and coordination, and facilitating routing information on a global scale.[103] MANRS also operates an observatory for monitoring routing incidents, providing visibility into a variety of routing security statistics, such as mis-originations, and route leaks.[104]

[93] NIST, NIST SP 800-189, Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation at 4, 12, 22 (2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189.pdf (*NIST SP 800-189*).

[94] *Id.* at 11, 14, 15.

[95] *Id.* at 7-8.

[96] NIST, *Robust Inter-Domain Routing Technical Details*, https://www.nist.gov/programs-projects/robust-inter-domain-routing/technical-details (last visited Apr. 10, 2024)(*Robust Inter-Domain Routing Technical Details*).

[97] NIST, *NIST RPKI Monitor* (Apr. 10, 2024), https://rpki-monitor.antd.nist.gov.

[98] *Robust Inter-Domain Routing Technical Details*

[99] *See, e.g.*, Stephen Kent, Charles Lynn & Karen Seo, Secure border gateway protocol (S-BGP), 18 IEEE Journal on Selected Areas in Communications 4582-92 (2000).

[100] Mutually Agreed Norms for Routing Security (MANRS), *RPKI Week*, https://manrs.org/resources/events/rpki-week/ (last visited Apr. 29, 2024); MANRS, *Routing Security Summit 2023*, https://manrs.org/event/routing-security-summit-2023/ (last visited Apr. 29, 2024).

[101] Internet Society, *Organization Members*, https://www.internetsociety.org/about-internet-society/organization-members/ (last visited Mar. 26, 2024); Internet Society, *Securing Global Routing*, https://www.internetsociety.org/action-plan/securing-global-routing/ (last visited Mar. 26, 2024).

[102] MANRS, *MANRS for Network Operators*, https://manrs.org/netops/ (last visited Mar. 26, 2024).

[103] MANRS, *Actions*, https://manrs.org/netops/actions/ (last visited Mar. 26, 2024).

[104] MANRS Observatory, *Overview*, https://observatory.manrs.org/#/overview (last visited Mar. 26, 2024).

On the same site, MANRS further provides views on the extent of deployment of RPKI-based measures and the recommended MANRS actions.[105]

33. The IETF is the principal standards development organization in the Internet arena, having been active since 1986.[106] In keeping with its role and history, it developed the first industry-driven standards to address security vulnerabilities in BGP in its Secure Inter-Domain Routing (SIDR) working group.[107] With the basic standards definition work in the SIDR WG deemed concluded, further standards work on the operational aspects of this subject matter continues in the IETF SIDR Operations (SIDROPS) working group.[108] In its Request For Comments (RFC) 6811, the IETF outlined the procedures for route origin validation using the RPKI distributed database.[109] RFC 8205 defines the BGPsec Protocol, where an extension to BGP provides security for the path of an AS by providing the AS with a BGP UPDATE message.[110] Most recently, IETF published a draft RFC, which is a work-in-progress detailing the use of ASPA objects in RPKI to verify BGP attributes of advertised routes, where the ASPA objects are cryptographically signed registrations of customer-to-provider relationships.[111]

## III. DISCUSSION

34. Today, we are seeking comment on several proposals targeted towards improving the security of Internet routing, in particular of BGP, which, as detailed above includes key vulnerabilities capable of impacting this nation's critical infrastructure. We intend these proposals to apply to providers of broadband Internet access service on a mass market retail basis (BIAS), based primarily on our authority under Title II of the Communications Act.[112] Our proposals take into account our understanding of the current state of industry participation in RPKI-based approaches to routing security, including the deployment of ROV, from our active and continuing engagement on these issues with industry stakeholders and other government agencies. In short, there is an apparent wide disparity in the percentage of originated routes covered by ROAs, and limited or incomplete support for ROV. Further action is urgently required.

35. As of March 2024, only 22% of U.S. networks allow for the validation of their routing information by registering and maintaining ROAs in the RPKI.[113] That figure is derived from data found

[105] *Id.*

[106] IETF, *Introduction to the IETF*, https://www.ietf.org/about/introduction/ (last visited Mar. 26, 2024).

[107] IETF Secure Interdomain Routing Operations (SIDR) working group, *Final Charter for Working Group*, https://datatracker.ietf.org/wg/sidr/about/ (last visited Apr. 29, 2024)(*SIDR Working Group*).

[108] *Id.*

[109] IETF, RFC 6811 - BGP Prefix Origin Validation at 3 (2013), https://www.rfc-editor.org/rfc/pdfrfc/rfc6811.txt.pdf.

[110] IETF, RFC 8205 - BGPsec Protocol Specification at 4 (2017), https://www.rfc-editor.org/rfc/pdfrfc/rfc8205.txt.pdf.

[111] IETF, BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects at 3 (2024), https://datatracker.ietf.org/doc/pdf/draft-ietf-sidrops-aspa-verification-17.(*BGP AS_PATH Verification*)

[112] *2024 Open Internet Order* at paras. 28, 125-26. We also seek comment on whether there are additional service providers that use BGP to route Internet traffic that should be included within the scope of this proceeding.

[113] MANRS provides a "readiness score" that describes the level that selected networks conform to MANRS, including whether the network helps validate their routing information by storing it in the RPKI. *See MANRS Observatory*, https://observatory.manrs.org/#/history (last visited Apr. 14, 2024)(filtering results by country and showing additional information regarding MANRS' measurements and scores in the information icons next to "MANRS Readiness" and "Routing Information (RPKI)"). More specifically, just over 22% of U.S.-based networks that participate in MANRS are RPKI "ready" or "aspiring" as of March 2024, according to MANRS measurements. *Id. NIST RPKI Monitor*, https://rpki-monitor.antd.nist.gov/ (last visited Apr. 14, 2024).

in the MANRS Observatory, and there are other measurement tools publicly available online that reveal similar data, such as NIST's RPKI Monitor.[114] The MANRS Observatory provides trend data for the maintenance of routing information in the RPKI by the networks participating in MANRS.[115] We observe that the use of RPKI services across the Internet has continued to increase over the past several years through service providers seeking to secure their BGP architectures.[116] Despite the increasing deployment of RPKI-based security measures by some service providers in the United States, service providers that participate in BGP routing will need to make additional progress to reduce exposure to the types of communications attacks described, and the ensuing risks.

36. Thus, consistent with comments filed by DOD, DOJ, and CISA in response to the *Secure Internet Routing NOI*, we are proposing certain requirements on service providers intended to help assess, prioritize, and maintain plans for utilizing the RPKI architecture to further BGP operational security.[117] As the agency with regulatory authority in this area, we intend to continue our close collaboration with other federal agencies which have been actively considering similar secure Internet routing issues through National Cybersecurity Strategy initiatives.[118] Our proposals are largely focused on the preparation and filing of BGP Routing Security Risk Management Plans, but we do seek comment on certain additional proposals that we believe hold promise for facilitating the implementation of RPKI-based routing security.

### A. BGP Routing Security Risk Management Plans

37. We propose to require service providers to prepare and maintain BGP Routing Security Risk Management Plans (BGP Plans) describing and attesting to the specific efforts they have made, and further plan to undertake, to create and maintain ROAs in the RPKI. The BGP Plans can be risk-based performance plans, but would have to describe and attest to the extent to which the service provider conducts ROV filtering at the interconnection points between the service provider and its peers and clients, as well as describe any other methods at their disposal. [119] These plans are to be updated on an annual basis. The following subsections discuss which service providers would be required to confidentially file their BGP Plans with the Commission, in addition to discussing the details that we propose should be included in all BGP Plans, whether filed with the Commission or not.[120]

#### 1. Initial BGP Plans

38. We propose to require certain large service providers to file initial BGP Plans with the Commission. BGP Plans submitted to the Commission are to be attested by a corporate officer at each service provider. In particular, we propose to impose this filing requirement on all Tier 1 service

[114] *Id.*; *NIST RPKI Monitor*, https://rpki-monitor.antd.nist.gov/ (last visited Apr. 14, 2024); *see also Cloudflare Radar*, https://radar.cloudflare.com/routing (last visited Apr. 14, 2024)(*Cloudflare Radar*); Hurricane Electric, *BGP Toolkit*, https://bgp.he.net/ (last visited Apr. 14, 2024); *APNIC Labs Measurements and Data*, https://labs.apnic.net/measurements/ (last visited Apr. 14, 2024).

[115] MANRS Observatory provides historical data collected over a one-year time span. *MANRS Observatory*, https://observatory.manrs.org/#/history (last visited Apr. 14, 2024).

[116] *See, e.g.*, *id.* (last visited Apr. 14, 2024)(showing increasing use of RPKI services since March 2022 among the networks that participate in MANRS).

[117] *See supra* para. 24; *see also infra* Sections III.A-C.

[118] *See infra* para. 107.

[119] Other methods include, for example, TCP-AO and peer-locking. IETF, RFC 5925 - The TCP Authentication Option at 4-5 (2010), https://datatracker.ietf.org/doc/html/rfc5925; Job Snijders, *Practical everyday BGP filtering with AS-PATH filters: Peer Locking*, North American Network Operators' Group, https://archive.nanog.org/sites/default/files/Snijders_Everyday_Practical_Bgp.pdf (last visited Apr. 15, 2024).

[120] *Infra* Sections III.A.1-3.

providers as well as the other most significant service providers, which would currently include: AT&T, Inc.; Altice USA; Charter Communications; Comcast Corporation; Cox Communications, Inc.; Lumen Technologies, Inc.; T-Mobile USA, Inc.; Telephone & Data Systems (including US Cellular); and Verizon Communications, Inc.[121] These significant providers are likely to originate routes covering a large proportion of the IP address space in the United States and will play critical roles ensuring effective implementation of ROV filtering. The initial BGP plans prepared by service providers other than those suggested above would not need to be filed with the Commission but should be made available to FCC staff upon request.

39. We seek comment on whether we should require the filing of BGP Plans by a different set of service providers than those identified above. If so, commenters should explain the reasons for, and factors involved with, reaching that determination, and the feasibility of using particular metrics. For instance, should only the most significant service providers based on number of clients, or number of public peers, need to file? Or, should we choose based on other criteria, such as several of the following: the size of the address space under their control (through legacy ownership or assigned by ARIN), the number of customers, or the number of originated routes?

40. We do not propose in this *Notice* to set specific industry-wide substantive requirements with industry-wide deadlines. Instead, BGP Plans are intended to establish a mechanism by which the Commission, working in coordination with other federal agencies, can assess a service provider's actions to prioritize routing security through use of the RPKI architecture, measure its progress over time to evaluate the reasonableness of its BGP routing security risk management plan, and verify its commitments to following it. In addition, the development of BGP Plans by all service providers would be important for securing BGP operations in the near term because it would require service providers to consider the benefits of creating and maintaining ROAs and conducting ROV filtering.[122] The specific BGP Plan requirements concerning ROAs and ROV are discussed *seriatim*.

### a. Creating and Maintaining Route Origin Authorizations

41. Registering and maintaining updated ROAs with the appropriate Internet registry is a critical and necessary step for securing BGP operation in the near term. At present, only the holders of specific IP address prefixes can register ROAs for originated routes that pertain to those prefixes.[123] As a result, a service provider is able to directly register and manage ROAs only when it controls the IP address prefix(es) in question.[124] An effective path forward must therefore take into account the

[121] We define "Tier 1" service providers as those that are able to reach all Internet end-points solely through peering relationships. *E.g.*, William B. Norton, *The Evolution of the U.S. Internet Peering Ecosystem*, North American Network Operators' Group 1, 2 (Nov. 19, 2003) https://archive.nanog.org/meetings/nanog31/presentations/norton.pdf (defining "Tier 1 ISP" as "an ISP that has access to the entire Regional Internet routing table solely through Peering relationships. Regional Tier 1 ISPs are at the top of the hierarchy and don't have to pay transit fees . . . All other ISPs operating in the region are required to purchase transit from one or more of the Regional Tier 1 ISPs").

[122] We are not proposing the rigid regulatory mandates feared by some. Letter from John Morris, Principal, U.S. Internet Pol'y & Advoc., Internet Society, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 23-320 et al., Attach. at 2 (filed Apr. 17, 2024). Rather, our preferred approach is to establish a framework that provides for a more informed and effective multistakeholder consideration of BGP security issues by government and industry stakeholders – one that enables a constructive path for timely addressing issues identified as hindering the deployment of the mature RPKI architecture.

[123] *See Resource Certification (RPKI)*(describing how resource holders use the RPKI architecture to attest to which ASNs should originate their IP address prefixes).

[124] *OECD Report* (citing Martin J. Levy, *RPKI – The required cryptographic upgrade to BGP routing* (Sept. 19, 2018), https://blog.cloudflare.com/rpki/). *See Route Origin Authorizations (ROAs)*, https://www.arin.net/resources/manage/rpki/roa_request/ (last visited Apr. 15, 2024). We use the term "control"

(continued….)

difference in the service provider's route origination control over the IP prefix(es) assigned to it by ARIN. The information we would require service providers to submit would depend on the various categories of IP address prefixes for which a service provider can be the route originator. In the subsections below, we discuss the different cases that we have observed in which the service provider either does or does not control the IP address prefix(es) assigned or allocated to it, and route originations for the same.[125] We anticipate that most service providers will be originating routes for prefixes drawn from all these cases. We would evaluate RPKI deployment in each set of circumstances differently depending on what type of control the service provider has over route originations to various IP address prefix(es).

#### (i) Cases Where the Service Provider Controls the ASNs and IP address prefix(es)

42. We first consider where a service provider has full authority to register ROAs because it controls the associated IP address prefix(es). ROAs are registered with the responsible regional registry, which is ARIN for the United States and North America.[126] ARIN assigns ASNs and IP address prefixes to the Local Internet Registries (LIRs).[127] As set out in the ARIN Manual, LIRs are "generally ISPs whose customers are primarily end users and possibly other ISPs."[128] The ISP might in turn designate a subset of the IP address space it holds to be used by its customers, but in the current ARIN operational convention only the original ISP can register ROAs even for reallocated address space.[129]

43. For these cases, we propose that BGP Plans would be required to include a detailed description of the service provider's process for assessing and prioritizing the creation and maintenance of ROAs which cover the routes originating from their networks. We contemplate that general statements that a service provider is following a risk-based approach would not be sufficient to satisfy the requirement for a detailed description. Rather, there need to be accountability mechanisms to ensure that each service provider takes meaningful action to assess its risk posture and that it prioritizes implementing protections accordingly. The BGP Plan would incorporate and explain in detail factors affecting the service provider's ability to register and maintain ROAs for its IP address prefix(es). We anticipate that a BGP Plan would include specific goals for the service provider pertaining to ROA registrations as well as estimated timetables for attaining those goals. We seek comment on what criteria providers should include in their BGP Plans for measuring progress in deployment of BGP origin validation, as well as what specific details should be provided to describe the service provider's plans for creating and maintaining ROAs going forward. We propose that the initial BGP Plans that are to be filed with the Commission should be filed no later than 90 days after the effective date of the requirement.

44. We seek comment on the criteria by which we should evaluate individual BGP Plans filed with, or reviewed by, the Commission. We recognize, for instance, that different service providers are in substantially different positions regarding the extent to which they control the ASN and the IP

colloquially. For purposes of this *Notice*, an entity controls the IP address prefix(es) when it is the only entity originating routes for it.

[125] The observations we note are derived from our Public Workshop and continued engagement with stakeholders.

[126] ARIN, https://www.arin.net/ (last visited Apr. 15, 2024)("ARIN is a nonprofit member-based organization that administers IP addresses & ASNs in support of the operation and growth of the Internet.").

[127] ARIN, *Number Resource Policy Manual* at 6 (Sept. 13, 2023), https://www.arin.net/participate/policy/nrpm/nrpm.pdf ("A Local Internet Registry (LIR) is an [Internet Registry] that primarily assigns IP addresses to the users of the network services that it provides.")(*ARIN Manual*).

[128] *ARIN Manual* at 6.

[129] An IP address space is a collection of one or more IP prefixes. *See* Xiaoqiao Meng et al., *IPv4 Address Allocation and the BGP Routing Table Evolution*, 35 Computer Communication Reviews 1, 71-72 (2005), https://escholarship.org/uc/item/8b46d4w4 (explaining how an IP prefix may represent an IP address block as allocated, a fragment of an allocated address block, or an aggregation of multiple allocated address blocks).

address prefixes that they originate. We also understand that some service providers have fewer in-house resources available than others. In addition, we anticipate receiving detailed explanations if a service provider contends that "multi-homing," traffic engineering, or some other factor significantly reduces its ability to increase and maintain ROA coverage for IP prefixes they control.[130] Regarding multi-homing, are there measures that would facilitate coordinating all necessary ROAs for all the ASNs that may originate routes to the same prefix? What are factors that might inhibit such coordination? If at least one ROA registration of the IP prefix is valid, is that sufficient to protect the IP prefix even if there are other invalid registrations for that prefix?

45. To help ensure that we are accurately measuring and tracking the status of ROA registrations, we seek comment regarding the metrics offered by several publicly available tools. The NIST RPKI Monitor is one example of these tools, but there are others available too.[131] We seek comment on the relative merits of such publicly available tools that track the status of ROA registrations covering route originations, including their utility in measuring providers' execution of their individual BGP Plans. Which, if any, are perceived to be more accurate or comprehensive than others? Should the FCC select one tool, based on comments submitted, to use to track ROA coverage? Or, should the FCC use a subset of public monitoring tools and cross-reference among them to track and analyze ROA coverage?

#### (ii) Cases Where the Service Provider Does Not Control the IP Address Prefix(es)

46. We next consider the information we propose to require in an initial BGP Plan in cases where we understand that service providers are unable to register a ROA because that service provider does not control the IP address prefix(es) in question. This apparently can happen in three instances: (1) A service provider can contractually reassign one or more IP address prefixes to downstream providers or other client customers, who are then the entities able to register ROAs for those prefixes.[132] (2) A party may obtain its own IP prefix directly from ARIN and use the service provider as its upstream provider. (3) A party may obtain its own ASN and IP prefix directly from ARIN and contract with the service provider to propagate the route. In those cases, we understand that the entity which controls the associated IP address prefix(es) in the RIR (ARIN), would have to register ROAs for those prefixes. In order to implement RPKI-based improvements to BGP security architectures successfully, and to create a healthy ecosystem, it is essential that every entity that controls IP address prefixes effects all necessary coordination to register the associated ROAs.

47. For these cases, we propose to require that a service provider's initial BGP Plan describe the status of the ROA registrations for routes they originate within these three cases. We propose that the BGP Plan explain the reason(s) why the service provider is unable to register particular sets of IP prefixes. The Plan should also describe in detail the service provider's efforts and plans for facilitating

[130] The term "multi-homing" refers to those cases where clients may use more than one upstream provider in order to ensure resiliency in connectivity to the Internet. *See* Ivan Novikov, *Decoding the Term: Deciphering the Significance of Multi-Homing?* (Nov. 17, 2023), https://securityboulevard.com/2023/11/what-is-multi-homing/ (detailing how ISPs use multi-homing to connect to multiple upstream providers, to ensure that their customers have uninterrupted access to the internet, even if one of the connections fails).

[131] *NIST RPKI Monitor*, https://rpki-monitor.antd.nist.gov (last visited Apr. 18, 2024); *see also* RIPE Labs, *BGPalerter*, https://github.com/nttgin/BGPalerter (last visited Apr. 15, 2024); *Cloudflare Radar*; Hurricane Electric, *BGP Toolkit*, https://bgp.he.net/ (last visited Apr. 15, 2024).

[132] *ARIN Manual* at 6 (defining the "reallocation" and "reassignment" of Internet number resources). A "reallocation" occurs when "IP addresses [are] delegated to an organization by an upstream provider for the purpose of subsequent distribution by the recipient organization to other parties." *Id.* A "reassignment" occurs when "IP addresses [are] sub-delegated to an organization by an upstream provider for the exclusive use of the recipient organization." *Id.*

the ROA registrations for the IP prefixes that have been transferred and not under its control. Among other issues, we believe that BGP Plans would need to describe the steps that the service provider takes to identify and address cases in which customers or clients with their own IP prefixes are multi-homed and the frequency it encounters multi-homing.[133] In multi-homing situations where it is the responsibility of the customer or client to create and register, rather than the service provider, the chances for errors in ROA registration may be greater, potentially resulting in the customer's traffic becoming blackholed through a given provider.[134] We understand that in many cases, the service provider will have direct contractual relationships with the holder of the IP address prefixes and will, or can be, made aware of the ROA registration status of those prefixes with ARIN.[135] Although the service provider itself is not able at this time to register ROAs in these circumstances, we are seeking comment on the steps that service providers can or should do to help secure ROAs for the IP address space held by downstream clients.[136]

### b. Route Origin Validation Filtering

48. The implementation of ROV is necessary to determine whether received route advertisements are legitimate when checked against ROAs in the RPKI repositories.[137] ROV is the step in origin validation predicated on the existence of ROAs, and is the key action that facilitates detection of invalid or unknown route originations that indicate a prefix is being incorrectly advertised, either maliciously or accidentally, by a service provider or enterprise network. For the RPKI to be effective, most if not all service providers will need either to conduct ROV filtering in their interconnections with other service providers, or to have contractual commitments with third parties to have routes propagated to them subject to ROV filtering.[138] Moreover, to fully realize the origin validation benefits of the RPKI, some service providers may need to perform ROV filtering in interconnections with their clients. In this way, the service provider examines incoming BGP routing announcements from its peers in addition to its clients. In cases where a service provider is downstream from a more widely accessed provider (e.g., stub networks), there could be great benefits from the downstream provider relying on the ROV filtering performed by its upstream provider.

49. The BGP Plan of a Tier 1 service provider should describe the extent to which it has implemented ROV filtering at its interconnection points with its peers as well as its customers, and to what extent ROV has been disabled or not deployed within its network. BGP Plans should also describe, to the extent applicable, any contractual requirements a service provider may have for upstream third-parties to provide ROV filtering for incoming routes.[139] We propose that this information would be required of all BGP Plans, whether filed with the Commission or made available upon request. We

[133] *Supra* para. 43.

[134] "Blackholing" occurs when an ISP drops traffic addressed to a targeted IP address or range of addresses by redirecting it to a null route. Imperva, *Blackholing*, https://www.imperva.com/learn/ddos/blackholing/ (last visited Apr. 15, 2024). Although blackholing is a technique used to mitigate effects from a DDoS attack, it can also occur as a result from both intentional and accidental routing incidents. *See id.*

[135] Issues regarding service provider contracts are discussed in detail below. *Infra* Section III.C.1.

[136] *See infra* Section III.C.

[137] Carlos Rodrigues & Vasilis Giotsas, *Helping build a safer Internet by measuring BGP RPKI Route Origin Validation* (Dec. 16, 2022), https://blog.cloudflare.com/rpki-updates-data.

[138] Symposium, Tomas Hlavacek et al., *Keep Your Friends Close, but Your Routeservers Closer*: *Insights into RPKI Validation in the Internet*, Advanced Computing Systems Association (USENIX) Security Symposium, 4841-58 (2023), https://www.usenix.org/system/files/usenixsecurity23-hlavacek.pdf ("The burden of protecting the global routing architecture primarily lies on large ISPs and Tier-1 providers. ROV implementation in Tier-1 providers greatly benefits Internet security as it limits the spread of hijacks to a localized scope.").

[139] *Infra* Section III.C.

believe that this information is likely to be most relevant for Tier 3 service providers who do not have peering relationships and solely rely on contracts with other upstream service providers.

50. We also seek comment on two proposals regarding the implementation of ROV filtering that potentially may affect the ROV information that needs to be included in certain providers' BGP Plans. We seek comment, first, on whether it would be sufficient if a Tier 1 service provider attests that it supports ROV for all directly connected peers with settlement-free access as well as their directly connected clients, including other service providers. We seek comment, second, on whether it would be sufficient if a Tier 2 service provider attests that it is implementing ROV filtering in peering relationships with other Tier 2 providers, and have contractual relationships with Tier 1 providers that require Tier 1 providers to perform ROV filtering on traffic being terminated to the Tier 2 provider. We seek comment as to whether there are circumstances where Tier 2 service providers need not provide ROV support for clients that participate in BGP routing. We also seek comment on the extent to which, if we adopt such proposals, ROV information needs to be included in a provider's BGP Plan.

51. We recognize that there are no publicly available resources that allow comprehensive third-party measurement and validation regarding the extent that service providers conduct ROV filtering. Third-party measurement methodologies involve some degree of sampling and estimation and come with varying strengths and weaknesses. For example, APNIC, Cloudflare, and Virginia Tech (RoVISTA), are examples of entities which have developed methodologies using various sampling techniques to assess the degree of ROV filtering prevalent, and which make the resulting assessments public.[140] We propose to monitor a limited set of respected consensus methodologies to determine whether the set, as a whole, shows consistent trends and patterns. We seek comment on whether there are particular approaches or sources that we should monitor for determining the extent to which an essential set of service providers is performing ROV filtering and executing on its BGP Plan.

52. We note that there are several publicly available, open-source software packages that validate BGP routing information based on information stored in the RPKI.[141] We seek comment on the maturity of the open-source software used in route validation, the degree to which these are currently deployed by service providers, the extent to which such deployments verify that secure software design principles including testing for trustworthy operation have been utilized, and the extent to which such software receives continued support by contributors. We seek comment on the inclusion of deployment decisions in the BGP Plan, to include mitigation plans in cases where the public domain software is no longer supported or available. We also seek comment on other validators not listed by ARIN.

### 2. Subsequent BGP Plans

53. We propose that subsequent BGP Plans do not need to be filed with the Commission by large service providers that attest that they have registered and maintained ROAs covering at least 90% of originated routes for IP address prefixes under their control. In other words, after the initial filings, large service providers that have at least 90% of the originated IP address prefixes that they control covered by active ROAs would not need to submit information about their process and future plans for assessing and prioritizing the creation and maintenance of ROAs in the RPKI, nor of their plans to conduct ROV filtering. Such a service provider, however, would be obligated to make its BGP Plan available to the Commission upon request from its staff. We anticipate that we may establish specific goals and deadlines

[140] APNIC Labs Measurements and Data, https://stats.labs.apnic.net/rpki (last visited Apr. 15, 2024); Cloudflare, *Is BGP Safe Yet?*, https://isbgpsafeyet.com/ (last visited Apr. 15, 2024); Virginia Tech, *RoVista*, https://rovista.netsecurelab.org/ (last visited Apr. 15, 2024).

[141] *Resource Certification (RPKI)*(describing how to obtain and install an RPKI Validator)(last visited Apr. 15, 2024).

for ROA registration in the future if progress is deemed insufficient after collaboration with federal interagency partners.[142]

54. We seek comment as to whether the 90% ROA coverage metric is a reasonable standard for determining when the large service providers identified above should no longer be required to file BGP Plans after the filing of their initial plans. Commenters disagreeing with use of that standard should propose an alternative standard, along with reasons why the alternative better serves the overall purposes of this proceeding.

55. We also seek comment on the content that needs to be included in the BGP Plans prepared after the initial Plans. We anticipate that subsequent Plans would largely consist of updates to the initial Plans, so that the burden of preparing such Plans would be significantly less than preparing the initial Plans. We seek comment on that conclusion and on what information should be included in subsequent Plans. We propose that the requirement to prepare subsequent BGP Plans annually would extend indefinitely, but seek comment on possible circumstances under which the preparation of BGP Plans would no longer be required of individual service providers or generally.

### 3. BGP Plan Issues for Service Providers Other Than the Largest Providers

56. As discussed above, we are proposing to require service providers other than the largest providers as defined in this *Notice* to prepare their BGP Plans generally in accordance with the same provisions.[143] Such service providers would not have to file their BGP Plans with the Commission but would still need to make them available to the Commission upon receiving a request from its staff. We believe that the development of a BGP Plan – even if never requested by the Commission – would be important for securing BGP in the near term because it would require service providers to consider the benefits of creating and maintaining ROAs and conducting ROV filtering.[144] We also think that those provisions generally take into account the different circumstances of various service providers.

57. Nevertheless, we also seek comment here on whether the information that these service providers would need to include in their BGP Plans should differ from the information required in the BGP Plans filed by the large service providers. If so, what information would not be needed, and why? In addition, to what extent should the required information change if they have maintained the 90% ROA threshold described above during the previous year?

58. We seek comment as well on whether to adopt significantly limited requirements for Tier 3 service providers – that is, those service providers that do not have peering relationships with any other providers and connect to the Internet only through upstream transit providers. What information should be included in the BGP Plans prepared by such Tier 3 service providers? For instance, would it be sufficient for their BGP plans to attest to all of the Org_ID information used in ARIN's WHOIS entries and to their ROA registration of their IP prefix(es), as well as to whether they have default BGP route(s) to their upstream provider(s) that all implement ROV on their traffic?[145]

## B. BGP Routing Security Information – Quarterly Reports

59. In addition to the preparation of BGP plans, we propose to require a set of the largest service providers as defined in this *Notice* to file specific data on a quarterly basis, which would be made

[142] *Infra* para. 76.

[143] *Supra* Section III.A.1.a.

[144] *See OECD Report* at 24 ("The usefulness of ROV filtering depends on the number of prefix holders that have created ROAs, and the accuracy of the ROAs themselves.").

[145] WHOIS is a distributed database populated by the RIRs (e.g., ARIN) whenever an organization receives an allocation of IP addresses from a RIR. *See* Leslie Nobile, *ARIN's Whois: What Data is Public Information and How Can it be Accessed?* (June 9, 2021), https://www.arin.net/blog/2021/06/09/arins-whois-what-data-is-public-information-and-how-can-it-be-accessed/.

publicly available by provider. We anticipate that such quarterly filings would allow the Commission to measure progress in ROA registration and maintenance and assess the reasonableness of the service provider's BGP Plan (not only on an industry-wide basis but also by individual and types of service providers). Tier 1 service providers would need to file the quarterly data described in the paragraph below, which would show the extent to which the service provider has maintained that coverage.[146] We propose that the first quarterly report be filed 30 days after the necessary steps are concluded to allow the relevant rule to take effect, and not from the date of publication of the adopted rule in the Federal Register.

60. We propose to include, and seek comment on including, the following information in quarterly reports concerning both legacy and ARIN allocated resources (i.e., ASN and IP prefix): (i) list of all Registry Org_IDs for all AS and address allocations to the service provider (obtained from WHOIS); (ii) list of all ASNs held by service provider; (iii) list of ASNs held by service provider that it uses to originate routes; (iv) list of address holdings that have been reassigned or reallocated;[147] (v) list of IP prefixes in originated routes that are covered by ROAs (grouped by originating AS number); and (vi) list of IP prefixes in originated routes that are not covered by a ROA (grouped by originating ASN). We seek comment as well on obtaining ROV-related data, including the extent to which ROV filtering is performed by the Tier 1 service provider for both directly connected peers with settlement-free access as well as their directly connected clients, including other service providers. We anticipate that much of the information requested would not vary by quarter, but that certain key data points related to ROA registrations could be tracked on a quarterly basis and would promote the Commission's ability to assess RPKI trends.

61. As noted above, there may be special challenges in the cases of ROAs for routes pertaining to networks that are multi-homed, and so the prevalence of such routes may well be relevant in assessing the security of the BGP routing system.[148] To what extent are service providers aware of multi-homing scenarios for the routes they originate, and can they enumerate and report on these use cases? Are there other sources of information on these cases? We believe that quarterly reporting is necessary, at least initially, to measure on a reasonably timely basis the evolution of RPKI-derived routing security, and to determine whether additional steps are needed—whether regulatory or otherwise—to encourage continued progress. We also believe that the data proposed for collection should be readily available within the individual service providers, and once collected, it should not be burdensome to be updated on a quarterly basis. For instance, ARIN repositories are updated every five minutes, and the NIST RPKI Monitor updates its analyses every six hours to reflect the corresponding route collector updates.[149] We seek comment on this approach.

62. In addition, this proposed direct reporting by service providers provides data, even though in the public domain, that is difficult, if not impossible, to reliably aggregate from publicly available sources. For instance, many service providers, especially the most widely accessed service providers, possess resources obtained from ARIN, including ASNs and IP address prefixes, under a wide variety of different Org IDs that are subject to change at any time. In addition, each publicly available measurement tool may have its own set of approaches and assumptions. We believe that direct reporting by a service provider of the requested information would not be burdensome because that information

[146] *Infra* para. 60.

[147] ARIN, *Reporting Reassignments*, https://www.arin.net/resources/registry/reassignments/ (describing allocations, assignments, reallocations, and reassignments)(last visited Apr. 15, 2024).

[148] *Supra* paras. 43, 47.

[149] *Resource Public Key Infrastructure (RPKI) FAQs & Best Practices*, https://www.arin.net/resources/manage/rpki/faq/#if-i-create-a-new-roa-when-will-it-be-published (last visited Apr. 26, 2024); NIST RPKI Monitor 2.0, *Methodology and User's Guide*, https://rpki-monitor.antd.nist.gov/Methodology (last updated Apr. 26, 2024).

should be readily available to it. Reporting that information would help ensure that Commission staff and the service providers are considering BGP progress from the same set of facts. We seek comment on these observations.

63. We further seek comment on the utility of requiring non-public information related to the above, including the following: (i) number of invalid routes received from peers and customers; (ii) proportion of invalid routes received relative to the total routes received per peer and customer; (iii) number of routes filtered in cases where the service provider itself implements RPKI-ROV; (iv) number of observed instances, if any, where RPKI-ROV processes were shown to incorrectly deem routes invalid due to inaccurate ROAs or other reasons; and (v) number of origin hijack instances pertinent to routes for service providers' address space that were (a) detected and (b) undetected during the reporting period.

64. Service Providers Other Than the Largest Providers. We propose that service providers other than the largest providers as defined in this *Notice* do not need to file quarterly data reports, and we have proposed significantly limited data reporting requirements to be included in their annual BGP Plans.

### C. Confidential Treatment of BGP Plans and FOIA

65. We plan to treat the BGP Plans as confidential under our rules; we tentatively conclude that such Plans will contain highly confidential and competitively sensitive business information that the companies would not publicly reveal, and may also contain trade secrets.[150] We seek comment on this conclusion, and on whether there are any other BGP routing security submissions that we might require that should be treated as confidential.[151] We note that, pursuant to section 0.461(d)(3) of our rules, when the Commission receives a request under the Freedom of Information Act (FOIA) for inspection of records that are presumed confidential or have been submitted with a request for confidential treatment, the custodian of the records shall provide a copy of the request to the submitter of the information, who will be given 10 calendar days to submit a detailed written statement specifying the grounds for any objection to disclosure.[152] If the submitter fails to respond, it will be considered to have no objection to disclosure.[153] We seek comment on whether this notice process is routinely necessary for filings with the Commission of BGP Plan reports or of any other submissions we conclude should be treated as presumptively confidential. In particular, should staff have discretion, upon consideration of all the circumstances, whether to initiate the notice process for any such reports or to deny such requests, other than from governmental entities that may be granted confidential access in connection with their official functions, outright? Is there any appreciable possibility, given the competitive sensitivity of the information contained in such reports and its potential misuse to cause network harm, that a submitter might not treat this information as confidential and object to its disclosure? If not, what is the benefit of routinely undertaking the notice process? Are there particular considerations, for example, the type of information requested within the reports or the stated public interest purpose for the request, that may militate in favor of disclosure after notice to the submitter? Are there objective criteria, such as the age of the reports, under which confirmation of the submitter's continued confidential treatment of the information and justification of its objection to disclosure should always be required?[154] Are there any legal limitations on our ability to withhold the reports under Exemption 4 of the FOIA without confirming

[150] *See* 47 CFR § 0.459(a)(3), (d).

[151] As stated above, however, we propose to make the quarterly reports filed by the largest providers publicly available. *Supra* para. 60.

[152] 47 CFR § 0.461(d)(3).

[153] *Id.*

[154] *See, e.g., Biles v. Dep't of Health and Human Services*, 931 F.Supp.2d 211, 225-27 (D.D.C. 2013)(rejecting claim of confidentiality, under formerly applicable competitive harm standard, in part because staleness of information rendered it of little value to submitters).

the submitter's objection to a specific information request?[155] We invite comment on these and any other questions relating to our affording confidential treatment to any such reports.

### D. Other Issues

#### 1. Possible Conditions on Service Provider Contracts

66. Based on our continuous engagement with industry and government stakeholders on BGP issues, we understand that a substantial portion of IP address prefixes issued by ARIN for the United States are prefixes for which service providers cannot register ROAs. As detailed above, these prefixes include circumstances in which the service provider has contractually reassigned IP prefixes received from ARIN to downstream providers or other client customers and therefore no longer controls the IP prefix for purposes of ROA registration. These cases also include circumstances in which the client customer has obtained the IP prefix (and possibly an ASN) directly from ARIN and therefore is the party able to register a ROA for those prefixes. In all these circumstances, we understand, the service provider has a contractual relationship with the holder of the IP address prefixes who is able to register ROAs with ARIN.

67. Given the substantial presence of these situations in the United States, it is critical that an overall strategy to address secure Internet routing issues develop and implement solutions that facilitate more widespread registration of ROAs for these prefixes—the foundational step necessary to enable RPKI -based BGP security measures towards securing the nation's communications from adversaries seeking to exploit BGP's inherent vulnerabilities, and thereby promote public safety and protect against serious national security threats. We propose above that BGP Plans address in detail the steps that a service provider is taking to address these issues. We continue to recognize as well the continuing importance of outreach and of education efforts. However, we are concerned that these steps may not be enough.

68. For instance, from our continuing stakeholder engagement, we understand that service providers believe that they are not in a position to insist in these situations that client customers register ROAs for these IP address prefixes. Unlike some Internet participants that have successfully adopted policies that require ROA registration for interconnection, service providers believe that they are not in a position to adopt similar policies and practices because client customers are likely to have alternative

[155] *See* 5 U.S.C. § 552(b)(4)(exempting from mandatory disclosure trade secrets and commercial or financial information obtained from a person and privileged or confidential); *see also Food Marketing Institute v. Argus Leader Media*, 588 U.S. 427, 434 (2019)(finding confidential treatment of information was established based on uncontested evidence of industry practice); U.S. Dep't of Justice, Office of Information Policy, *Exemption 4 After the Supreme Court's Ruling in Food Marketing Institute v. Argus Leader Media*, https://www.justice.gov/oip/exemption-4-after-supreme-courts-ruling-food-marketing-institute-v-argus-leader-media (advising that agency may determine information is treated as confidential based on its own knowledge of industry practice and nature of the records as well as on specific information from the submitter); Executive Order 12600, Predisclosure Notification Procedures for Confidential Commercial Information, 52 Fed. Reg. 23781 (June 23, 1987)(directing agencies to promulgate procedures to notify submitters of records containing confidential commercial information when those records are requested under the FOIA if the agency determines it may be required to disclose the records). The courts are divided as to whether, and the extent to which, the FOIA requires a showing of foreseeable harm other than the loss of confidentiality itself to support the withholding of information under Exemption 4. *See* 5 U.S.C. § 552(a)(8)(A)(i)(agency shall withhold information only if the agency reasonably foresees that disclosure would harm an interest protected by an exemption or disclosure is prohibited by law); *compare, e.g., Seife v. U.S. Food and Drug Administration*, 43 F.4th 231, 240-42 (2d Cir. 2022) (requiring harm to the submitter's commercial or financial interests) *with American Small Business League v. U.S. Dep't. of Defense*, 411 F.Supp.3d 824, 835-36 (N.D. Cal. 2019) (finding loss of confidentiality to constitute sufficient harm). To the extent something more than the loss of confidentiality is required, does the nature of the information in BGP-related reports, including its competitive sensitivity and its implications for network security, support a *per se* finding of harm from its disclosure?

options for their upstream service provider who would not insist that the IP address holder take the additional step of registering ROAs.

69. Because the benefits that the RPKI-based approach to a more secure BGP can contribute to national security are so great, we must consider all possible tools and options at our disposal in order to address these potential collective action issues. We therefore are seeking comment on the additional proposals below, which we believe to be in line with the whole-of-government approach to "develop and drive adoption of solutions that will improve the security of the Internet ecosystem and support research to understand and address reasons for slow adoption."[156]

70. In particular, we seek comment on possible conditions that the Commission should place on current and future contracts entered into by service providers. There are three separate cases to consider in this context: (i) where the IP address prefix was originally held by the service provider holding the ASN, who then reallocated/reassigned the prefix to a client; (ii) where the IP address was obtained directly from ARIN by the client; and (iii) where the service provider is propagating routes where the client has obtained both the ASN and the IP address prefixes that are to be originated.

71. We seek comment in such cases on the possibility of the following conditions to address cases where the service provider does not hold the IP address prefix in a route without a corresponding ROA: (i) prohibiting entry into new contracts unless those contracts contain plans for registering ROAs for the originated routes; (ii) requiring service providers to insist on ROA registrations by existing clients with IP prefixes it has transferred to them, or to "take back" any IP prefixes it has leased to clients; and (iii) requiring service providers, at the time of contract renewal (or after a set period, such as two years), to insist on having a plan for ROA registration from their client.

72. Again, we seek to address any potential for collective action issues under these circumstances. Would a service provider or its customer be likely to encounter any disincentives for the registration of ROAs, particularly if, in the absence of any conditions, other service providers are free not to do so? We seek comment on the likelihood that a service provider might lose customers if it wanted to require ROA registration (and/or ROV filtering) to be implemented by their peering or downstream neighbor. Assuming that a peering or downstream service provider (e.g., Tier 3 provider) might well choose a different transit provider to connect their customers to the Internet if the alternate transit provider did not require the downstream service provider to register and maintain accurate ROA objects pertaining to its IP address prefixes, to what extent can providers of transit or other interconnectivity services incorporate mandatory language into the corresponding contractual agreements?

73. To address these potential collective action barriers to widespread ROA registration, we seek comment on requiring that providers' contracts in these cases to provide for the registration of ROAs for the relevant IP address prefixes. For instance, as identified above, we seek comment on requiring service providers not to enter into new contracts to route traffic unless ROAs are registered for the relevant IP address prefixes. Should such contracts also require the holder of the IP prefix to maintain the active ROAs? We also seek comment on requiring service providers to mandate that clients with whom they have a direct contractual relationship to register their IP prefixes with ARIN. If a client refuses to register assigned prefixes, could a service provider "take back" unregistered IP address prefixes it has leased to others so as to enable the service provider to register ROAs for those prefixes? We recognize possible disruptions in certain cases that may outweigh the benefits, and so seek comment on imposing certain requirements at the time of contract renewal. In order to judge the potential benefits and costs of

[156] *Biden NCSIP* at 38; *see also Biden NCS* Exec. Summary ("This strategy recognizes that robust collaboration, particularly between the public and private sectors, is essential to securing cyberspace."); *Biden NCS* at 23-24 ("We can build a more secure . . . digital ecosystem through strategic investments and coordinated, collaborative action. . . . However, public and private investments in cybersecurity have long trailed the threats and challenges we face. . . . We must take steps to mitigate the most urgent of these pervasive concerns such as [BGP] vulnerabilities[.]").

any such requirements, we seek comment on whether general industry standards exist for setting the term of any such contracts. We also recognize that any such requirement would depend on the provisions and terms of the existing contracts, as well as when their contracts are set to renew. We further seek comment on the percentage of client contracts that extend beyond two years of the publication of this proceeding. For instance, if a substantial percentage of contracts are five years or longer, should the Commission consider imposing requirements no later than a set time period, such as two years from the effective date of the adoption of rules.

74. In summary, we seek comment about the benefits and drawbacks of considering these and any other regulatory approaches to encourage the creation and maintenance of ROAs in the RPKI through contractual requirements between service providers and their customers, and the provisioners of Internet resources.

### 2. Possible ROV and ROA Requirements for Service Providers

75. We have sought comment above on whether the ROV implementation content of the BGP Plans of Tier 1 and Tier 2 service providers should differ depending on whether they are able to attest to certain ROV implementation.[157] We here seek comment on proposals to require certain levels of implementation of ROV by Tier 1 and Tier 2 service providers. In particular, we seek comment on whether Tier 1 service providers should be required to achieve the ROV deployment described above within one year of the effective date of such a requirement, and whether Tier 2 service providers should be required to achieve the ROV deployment described above within two years of the effective date. As described above, ROV implementation is a critical piece of successful RPKI implementation, and we believe that those target dates are reasonable given the current state of ROV deployment.

76. In the sections above we propose that the largest service providers prepare and file BGP Plans that address the service providers' plans for registering and maintaining ROAs in the RPKI.[158] Here, we seek comment on whether the Commission should establish goals and timelines for the largest service providers to register ROAs covering the routes they originate. If so, how should the Commission determine reasonably achievable goals and timelines for service providers? What factors should we consider in making those determinations? Should we set goals and timelines on an individualized basis for the largest providers dependent on the service provider's individual circumstances? To what extent should the registration of certain ROAs in the RPKI be prioritized, and what should be the basis for identifying those ROAs and defining reasonable prioritization? Can we set meaningful goals and/or timelines on a standardized basis for those providers or for all service providers subject to this *Notice*? Is there a floor below which ROA registration levels should raise particular concern regarding whether ROAs registrations are being timely deployed? If so, commenters should provide specific suggestions, along with justifications.

### 3. Outreach and Education

77. We see a clear need for additional education efforts by the service providers, various stakeholder groups, ARIN, and governmental entities. As described below, we believe that a number of holders of IP address prefix(es) do not fully appreciate the importance of registering ROAs for their IP address prefix(es) to help protect those critical resources from being compromised in the Internet routing system, with potentially disastrous consequences described in the examples above. Education about the substantial benefits of registering ROAs is a necessity. To what extent can or should large service providers as defined in this *Notice* take steps to support ROA registration by other, downstream providers? We also think it is important to increase the options for holders of IP prefixes to register ROAs for those prefixes.

[157] *Supra* para. 50.

[158] *Supra* Section III.A.

78. We seek comment in this context on steps we should consider to facilitate the creation and maintenance of ROAs in the RPKI. There are resources available to help entities of all sizes. For example, the RIRs provide guidance to help populate RPKI, including the registration and maintenance of ROAs.[159] We seek comment on the extent to which such implementation guidance and resources help service providers of all sizes create and maintain ROAs over the IP address(es) that they originate from their networks. Are there any aspects that would be better served or supported by a government-led educational campaign seeking to drive awareness of the issue and facilitate increases in the proportions of ROAs to route originations in the RPKI repositories? If so, would the inclusion of our federal partners, for example, CISA, NIST, and ONCD in such a campaign, facilitate driving both awareness of the seriousness of the issue, as well as provide educational support for the process involved with accurately registering and actively maintaining ROAs in the RPKI infrastructure? What would the metric for "success" be for such an educational campaign? Should we request volunteers to join workshops to encourage and facilitate the creation and maintenance of ROAs? Additionally, how should we treat those cases where a downstream service provider holds its own or reassigned IP address space?

79. We separately seek comment on the extent to which a government-led educational campaign could facilitate service providers increasing their level of ROV filtering on their own networks. Should we consider the relative size of the service provider in addition to the Tier category to which it might be considered to belong? Should such a campaign educate on both ROV filtering and ROA object registration and maintenance, or should they target them as separate campaigns? What would a metric for "success" be for such an educational campaign? Should we request volunteers to join workshops to encourage and facilitate the use of ROV filtering on certain parts of the networks they control?

### 4. ARIN Processes

80. ARIN is the RIR serving the United States and other countries within its coverage area.[160] It maintains a RPKI repository publication point, offers hosted RPKI services, and is the source from which would-be resource holders/network operators/service providers within the United States obtain Internet number resources, such as ASNs and IP addresses. ARIN is also the entity that enables U.S. service providers to register, update, and publish ROAs. Beyond providing additional educational materials, conducting workshops, and outreach, ARIN has at least two initiatives that could facilitate the uptake of RPKI-based routing security measures: (i) ARIN had referred for community consultation a question from one of its members, that was filed in the form of a ticket, asking if reassigned address space holders can register their prefixes with ROAs, and thus take advantage of the benefits of RPKI origin validation; and (ii) ARIN is considering changes in its ROA creation processes to flag instances where attempted ROA registrations raise the possibility of misconfigurations.[161] We seek comment on the role that these two initiatives may play in facilitating ROA registration, and on whether there are any other steps ARIN can take to encourage implementation of the RPKI.

### 5. Beyond RPKI Origin Validation – Further Efforts to Secure Internet Routing

81. Although the regulations proposed with this *Notice* focus on securing route origination, we seek comment on techniques and architecture towards path validation as well. Path validation ensures

[159] *Resource Certification (RPKI*); RIPE Labs, *Tools and Resources*, https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/tools-and-resources/ (last visited Apr. 15, 2024); APNIC, *RPKI*, https://www.apnic.net/community/security/resource-certification/ (last visited Apr. 15, 2024).

[160] ARIN, *Our Region*, https://www.arin.net/about/welcome/region/ (last visited May 3, 2024).

[161] ARIN, *ACSP Suggestion 2023.8: Allow Customers with reallocated resources to create ROAs* (June 27, 2023), https://www.arin.net/participate/community/acsp/suggestions/2023/2023-08/; ARIN, *Results of Consultation on RPKI/BGP Intelligence* (Mar. 11, 2024), https://www.arin.net/announcements/20240311/.

the integrity and authenticity of the AS Path attribute.[162] The only standard designed to address issues with path validation and plausibility is BGPsec.[163] Implementing this is challenging due to the intensive cryptographic operations involved. A less complete guarantee on path security is offered by a work-in-progress effort from the IETF, known as autonomous system provider authorization (ASPA).[164] This effort is designed to detect invalid BGP AS_PATHs by registering ASPA objects in the RPKI containing verifiable, attested information as to probable ASNs in the path. In addition, the ASPA approach accommodates incremental deployment, and "provides benefits to early adopters in the context of limited deployment." These methods, however, are still undergoing discussion among the academic and standards community and are not ready for implementation.[165] Although this *Notice* focuses on issues with origin validation and the techniques currently available to address them, achieving a truly secure routing system will involve steps beyond deploying RPKI-based origin validation. We do not propose at this time to require service providers to implement measures to address path validation, but we note that their implementation is expected to be a critical, future step that service providers would need to take to secure their routing systems. We seek comment on the maturity of this work-in-progress and any anticipated timeline in which ASPA can be deployed after it has been standardized.

## E. Benefits and Costs

82. We seek information on the potential benefits and costs of our proposals. We estimate our proposals would result in billions of dollars of benefits through various channels, which exceeds our upper bound estimate of annual costs of $30.8 million. Below, we present estimates of these benefits and costs and seek comment on these costs and benefits, as well as the proposed data sources and methodology.

### 1. Benefits

83. As stated earlier, adversaries can exploit BGP security vulnerabilities that can lead to substantial public harms.[166] In addition to criminal activity, poor BGP security can lead to threats to national security or damage to critical infrastructure. Thus, improving the security of BGP would have substantial benefits from reducing the rate of such incidents.

84. *Implementing BGP Routing Security Risk Management Plans and BGP Routing Security Quarterly Reports*. While we believe that it is impossible to quantify the precise dollar value of improvements to the public's safety, life, and health, as a general matter, we nonetheless believe that very substantial public safety benefits will result from the BGP Routing Security Risk Management Plans and BGP Routing Security Quarterly Reports we propose today.[167] By implementing BGP Plans and submitting quarterly data reports, service providers will be better able to ensure that Internet traffic routed through their networks is secure and will not be subject to unlawful interference, thus preserving public trust and better protecting national security and public safety. As a consequence, we anticipate that the rule changes we propose today will yield substantial cybersecurity benefits.

85. Independent of that analysis and as presented in the *2022 Alerting Security NPRM*, "the Commission has previously found that "a foreign adversary's access to American communications

[162] *NIST SP 800-189* at 22, 23.

[163] *SIDR Working Group*; *see also BGP AS_PATH Verification*; *see also OECD Report* at 21, 29.

[164] *SIDR Working Group*; *BGP AS_PATH Verification*.

[165] *See, e.g.*, *OECD Report* at 21 ("However, [BGPsec and ASPA] are still under discussion and not ready for implementation.").

[166] *See supra* paras. 7-12.

[167] *Cf. Resilient Networks*, Report and Order, PS Docket 21-346, 37 FCC Rcd 8059, 8075, para. 46 (2022) (*Resilient Networks Order*)("[I]t would be impossible to quantify the precise financial value of these health and safety benefits[.]").

networks could result in hostile actions to disrupt and surveil our communications networks, impacting our nation's economy generally and online commerce specifically, and result in the breach of confidential data.""'[168] Our annual national gross domestic product was nearly $23 trillion in 2021, adjusting for inflation.[169] Accordingly, if extending the requirement to create and implement BGP Plans and BGP Routing Security Quarterly Reports plan to additional providers prevents even an additional 0.005% disruption to our economy, we believe the cyber risk management plan certification requirement we adopt today would generate $1.15 billion in annual benefits. Likewise, the digital economy accounted for $3.31 trillion of our economy in 2020, and so we believe preventing a disruption of even 0.05% would produce annual benefits of $1.66 billion.[170] As a check on our analysis, consider the impact of existing malicious cyber activity on the U.S. economy: $57 billion to $109 billion in 2016.[171] Given the incentives and documented actions of hostile nation-state actors, reducing this activity (or preventing an expansion of such damage) by even 1% would produce annual benefits of $0.57 billion to $1.09 billion. Given this analysis, we believe the benefits of our rule to the American economy, commerce, and consumers is likely to be substantial. Does this analysis apply, or does it need to be modified or replaced to be more relevant to the proposals contemplated here? We seek comment on this analysis and ask commenters to be specific by providing data to illustrate the benefits our proposed rules would have to national security, public safety, and the economy.

### 2. Costs

86. We estimate an upper bound of $30.8 million in annual costs for our proposed requirements. These costs would come from developing and filing BGP routing security management plans ($16 million), filing BGP routing security reports ($2,000), quarterly filing requirements ($74 thousand), and from new registrations that may result from possible Tier 1 service provider ROV support requirements and required conditions on service provider contracts ($14.7 million).

87. *BGP Routing Security Risk Management Plans.* We propose the service providers must maintain and possibly file an Annual BGP Routing Security Risk Management Plan. The largest providers, which include all Tier 1 providers and some additional large providers of interest, must file their plans with Commission initially.[172] They must then file plans annually if they cannot attest that they have registered and maintained ROAs covering at least 90% of originated routes for IP address prefixes under their control.

88. We estimate an annual upper bound cost for the BGP Routing Security Risk Management Plans to be $16 million. We have no firm estimate of how many service providers maintain plans currently, so as an overestimate, we estimate 80% of firms would develop and maintain plans that

[168] *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, et al.*, PS Docket No. 22-329, Notice of Proposed Rulemaking, 37 FCC Rcd 12932, 12947, para. 31 (2022); *see also China Telecom (Americas) Corporation Order on Revocation and Termination*, Docket No. 20-109, Order, 36 FCC Rcd 15966, 16019-20, para. 81 (2021).

[169] *See* Press Release, Bureau of Economic Analysis, U.S. Department of Commerce, Gross Domestic Product (Third Estimate), Corporate Profits (Revised Estimate), and GDP by Industry, First Quarter 2022 (June 29, 2022), https://www.bea.gov/sites/default/files/2022-06/gdp1q22_3rd.pdf.

[170] *See* Tina Highfill & Christopher Surfield, Bureau of Economic Analysis, U.S. Department of Commerce, *New and Revised Statistics of the U.S. Digital Economy, 2005-2020* (May 2022), https://www.bea.gov/system/files/2022-05/New%20and%20Revised%20Statistics%20of%20the%20U.S.%20Digital%20Economy%202005-2020.pdf.

[171] *See* The Council of Economic Advisers, The Cost of Malicious Cyber Activity to the U.S. Economy at 36 (Feb. 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[172] *Supra* para. 38. This category currently includes: AT&T, Inc.; Altice USA; Charter Communications; Comcast Corporation; Cox Communications, Inc.; Lumen Technologies, Inc.; T-Mobile USA, Inc.; Telephone & Data Systems (including US Cellular); and Verizon Communications, Inc.

otherwise would not. Based on Form 477 data, we estimate there are 2,209 service providers.[173] We estimate that creating and maintaining a plan would entail 100 work hours from a technical manager, whom we estimate are compensated at $90.16/hour.[174] Our upper bound annual BGP routing security risk management plan development and maintenance cost is then $15,933,075 (=80% × 2,209 service providers × 100 hours × $90.16/hour) which we round to $16 million to avoid a false impression of precision. Costs in subsequent years would be lower than the first year because they would only include maintenance, and not plan development. Therefore, we use the cost of the first year as an upper bound for subsequent years as well.

89. We estimate an upper bound of a risk management plan filing cost of $2,000. Only the largest service providers, with customers in the millions or high hundreds of thousands, would need to file. Consulting Form 477 subscriber numbers, internal staff calculations suggest that 20 is a reasonable estimate for the number of large providers.[175] However, as stated above, nine service providers are currently in this category that requires filing.[176] We estimate filing plans would take a general manager 1 work hour, and, again, we estimate that this general manager is compensated at $90.16/hour.[177] In subsequent years, not every service provider must file, so as an upper bound on cost for a typical year we use the cost of the first year. The upper of bound of this filing cost is then $1,803.20 (= 20 service providers × 1 hour × $90.16/hour) which we round to $2,000 to avoid a false impression of precision.

90. We seek comment on the assumptions underlying these cost estimates, especially the number of service providers affected, the work hours involved and the appropriateness of the assumed compensation. We also seek any information on the identities of the service providers that should be considered large, and whether 20 is a reasonable estimate for the number of service providers required to file.

91. *BGP Routing Security Information – Quarterly Reports.* We propose the largest service providers would need to file quarterly reports on BGP routing security. We believe these filing and development costs are analogous to the filing costs for the risk management plans, so we elect to use the same methodology for these costs, adjusting for the quarterly rate of submission and the fact the quarterly report would likely take less time to create than full plans. We decrease the assumed work hours for developing each report to 40 from 100, but keep filing time and the hourly compensation the same.[178] We therefore estimate an annual upper bound cost of these quarterly filings to be $73,931 (= 4 reports/year × 20 service providers × (40 hours of report development + 1 hour of filing) × $90.16/hour), which we

[173] *See* FCC, *Broadband Data Collection, Data Specifications for Biannual Submission of Subscription, Availability, and Supporting Data* (Mar. 30, 2023), https://us-fcc.app.box.com/v/bdc-availability-spec (*Broadband Data Collection*).

[174] We assume similar cybersecurity plans would take 100 work hours. We estimate total compensation for technical managers as $92.16/hour =$62.18/ hour × 145%. *See* Bureau of Labor Statistics, *Occupational Employment and Wages, May 2023, 11-1021 General and Operations Managers* (Apr. 3, 2024), https://www.bls.gov/oes/current/oes111021.htm (*General and Operation Managers Mean Hourly Wage*) (mean hourly wage is $62.18 for occupation code 11-1021 General and Operations Managers). According to the Bureau of Labor Statistics, as of September 2023, civilian wages and salaries averaged $30.35/hour and benefits averaged $13.58/hour. Total compensation therefore averaged $30.35 + $13.58 = $43.93. *See* Press Release, Bureaus of Labor Statistics, Employer Costs for Employee Compensation – September 2023 (Dec. 15, 2023), https://www.bls.gov/news.release/pdf/ecec.pdf (*Compensation Benefit Mark-up*). Using these figures, benefits constitute a markup of $13.58/$30.35 = 45%. We therefore markup wages by 45% to account for benefits.

[175] *See Broadband Data Collection*.

[176] *Supra* para. 38

[177] We assume filing incident reports would take 1 work hour. *See General and Operation Managers Mean Hourly Wage*; *see also Compensation Benefit Mark-up.*

[178] *See General and Operation Managers Mean Hourly Wage* and *Compensation Benefit Mark-up.*

round to $74 thousand to avoid giving a false impression of precision. We seek comment on the assumptions underlying these cost estimates, especially the number of service providers affected, the work hours involved and the appropriateness of the assumed compensation.

92. *Conditions on Service Provider Contracts and Possible ROV and ROA Requirements.* We estimate an upper bound of $14.7 million of annual cost from potential conditions on service provider contracts and ROV and ROA requirements for Tier 1 and Tier 2. Ideally, if these measures are successful, all non-registered IP addresses would become registered. Complete registration is an overestimate of the true effect, especially since ROV and ROA requirements would be for Tier 1 and Tier 2 providers only, but we will assume this to form an upper bound on costs associated with registration. To achieve this, we assume non-compliant service providers and network service providers must implement RPKI architecture which is a costly endeavor.

93. FCC staff estimates indicate that a total population of 2,209 service providers would fall under the purview of a potential order.[179] Costs of implementation and current compliance with RPKI would vary based on the size of the subscriber base of each ISP and service provider, so we approximate by separating the service providers, for our analytic purposes, into large, medium and small service providers. Consistent with the rest of our analysis we assume 20 large service providers, and we assume there are approximately 30 medium service providers which corresponds to hundreds of thousands of subscribers.[180] The remaining 2,159 service providers we designate as small. Based on internal staff analysis of the required labor and material costs, we approximate the per-service provider cost of larger service providers to be $314,380, of medium service providers to be $65,752, and small service providers to be $22,588.[181] We believe that most large providers already have RPKI architecture, so we approximate that only 30% of large providers would implement RPKI architecture. Medium service providers likely have less compliance so we assume 50% of medium service providers would have to implement. The vast majority of small providers do not own their own ASNs, so would likely not need to comply with RPKI infrastructure. We therefore assume 5% of small providers would have to comply, which is likely an overestimate. Taking these numbers together, we estimate that service provider costs would total $5,310,978 (=(20 large service providers × $314,380 × 30%) + (30 medium service providers × $65,752 × 50%) + (2,159 small service providers × $22,588 × 5%)), which we round to $5.3 million to avoid a false impression of precision.

94. Given that the FCC lacks a dedicated information collection on network service providers, we have a less definite breakdown of the number of affected services. Many larger service providers are also large network service providers so we have already counted them, and most small service providers would not have ASNs so would not need to comply. To approximate the number of

[179] *See Broadband Data Collection*.

[180] *Id.*

[181] To approximate labor costs, we assume the wage of a senior network engineer, which we approximate through the hourly wage of Computer Network Architect at the 75th percentile of the wage distribution, $78.88/hour. *See* Bureau of Labor Statistics, *Occupational Employment and Wages, May 2023, 15-1241 Computer Network Architects* (Apr. 3, 2024), https://www.bls.gov/oes/current/oes151241.htm. We estimate total compensations as $114.38/hour by multiplying $78.88/hour by 145% to account for benefits. *See Compensation Benefit Mark-up.* Larger service providers require more work hours to complete RKPI implementation, so staff assumes a large network would take 1000 work hours, a medium network would require 400 work hours and a small network would require 180 work hours. Likewise large service providers would require more specialized equipment and software licenses to handle large amounts traffic and therefore incur much more material costs. A small service providers needs only a server and open source tools for the small amount of traffic it has. We therefore estimate a large service provider would incur $200,000 in material costs, a medium service provider $20,000, and a small service provider $2,000. Taken together, a large, medium and small service provider would have total costs of $314,380 (=(1000 work hour× $114.38 /hour) + $200,000), $65,752 (=(400 work hour× $114.38 /hour) + $20,000) and $22,588(=(180 work hour× $114.38 /hour) + $2,000), respectively.

network service providers, we then use the number of medium service providers, but we assume 100% non-compliance, which likely overestimates the number of medium network service providers in non-compliance but accounts for the non-compliant large network service providers and small network service providers. To further ensure that our cost estimate is an overestimate, we assume the compliance cost of large service providers is $314,380. Thus we estimate an upper bound of total network service provider cost to be $9,431,400 (=30 service providers × $314,380), which we round to $9.4 million to avoid a false impression of precision

95. Under the tentative assumption that the possible contract conditions cause no change in traffic patterns, we believe that there are no additional costs. While additional contract terms would potentially change transaction terms between service providers and the IP address holders, any loss from a party would be cancelled out by its transfer to another party. The other possible costs would be from changes in traffic patterns, in either through which service providers they are routed or changes in the total amount of traffic. If these new terms caused parties to shift business away from their ideal contracting partner, that could lead to a loss in efficiency. We tentatively assume that possible contract conditions would be universal to all contracts, and so would impact each potential pair of transacting server providers equally. Further, we do not expect any less total traffic, as the Commission estimates that demand for Internet service from IP address holders is more or less inelastic, as traffic demand is largely in the hands Internet users. We seek comment on the reasonableness of assuming no further change in traffic, especially whether contract conditions would have disparate impacts on different service providers and network service providers.

96. Combining the total service provider ($5.3 million) and network service provider costs ($9.4 million), we estimate the upper bounds of total cost from possible changes to contract conditions to be $14.7 million. This cost would be spread over several years as current firms come into compliance gradually. We anticipate modest entry of new service providers after the initial ramp-up in compliance, so costs incurred by firms that do not currently exist would be modest. We also anticipate that maintenance costs likely would be nominal in comparison to the costs of the original ramp-up. We therefore use the $14.7 million as an upper bound of annual costs.

97. We seek comment on these estimates of possible changes to service provider contract conditions. Is our characterization of how costs would be incurred and who would incur them reasonable? Are our estimates of the levels of costs for different service providers reasonable? Is our assumption that most small providers would not build their own solutions reasonable? Are our assumptions that traffic would not change reasonable?

### F. Legal Authority

98. We find the Commission has authority to adopt the proposed BGP measures. We base this finding on a number of different statutory provisions, including the Commission's obligation to consider the public interest in our regulation of common carriers under Title II, and of radio communications under Title III.[182] As discussed most recently in the *2024 Open Internet Order,* such public interest analysis incorporates the core statutory purposes for the creation of the Commission—the national defense and the promotion of the safety of life and property.[183]

99. Title II of the Communications Act of 1934, as amended (Act) grants the Commission authority to consider the national defense as it considers whether practices of common carriers are unjust, unreasonable, or unreasonably discriminatory.[184] With the reclassification of BIAS as a

[182] 47 U.S.C. §§ 151, 201-202, 301.

[183] *See* 47 U.S.C. § 151; *2024 Open Internet Order* at paras. 342, 431.

[184] *2024 Open Internet Order* at para. 29 ("Upon today's reclassification of BIAS as a Title II telecommunications service, we rely on our authority in sections 201 and 202 of the Act, along with the related enforcement authorities

(continued….)

telecommunications service, the providers of such services are subject to Title II under the terms of the *2024 Open Internet Order.*[185] Under Title II of the Act, the Commission is obligated to ensure that "[a]ll charges, practices, classifications, and regulations" in connection with common carrier services must be "just and reasonable."[186] Furthermore, section 201 authorizes the Commission to prescribe rules and regulations necessary in the public interest to carry out the provisions of the Act.[187] In this context, the proposed requirements for RPKI implementation aim to guarantee secure and reliable telecommunications services in the form of secure Internet routing and cybersecurity[188]

100. The Commission's Title III authority allows it to impose license conditions related to BGP Plans and BGP Routing Security Quarterly Reports and disclosures on wireless licenses. Title III empowers the Commission to establish conditions, terms, and requirements for wireless licensees, including providers of commercial mobile service, which we tentatively conclude covers regulations that promote the security and reliability of wireless networks.[189] Of particular relevance, section 303(b) directs the Commission, consistent with the public interest, to "[p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class."[190] By requiring cybersecurity efforts around RPKI, we propose to enable the Commission's ongoing review of threats over wireless networks and disruption to the nation's alerting systems, which in turn would contribute to greater reliability and effectiveness going forward.

101. Further, section 706 of the Telecommunications Act of 1996 may provide additional support for the cybersecurity safeguards we propose today.[191] Section 706 of the 1996 Act requires the Commission to inquire whether "advanced telecommunications capability is being deployed to all Americans in a reasonable and timely fashion."[192] Section 706 defines "advanced telecommunications capability" as including "high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology."[193] Section 706, while worded in terms of encouraging the deployment of 'advanced telecommunications capability,' has long been understood to encompass the goal of encouraging broadband Internet access, and our proposed measures, which are designed to promote more secure Internet routing, should also encourage that objective. Additionally, section 706 directs the Commission

of sections 206, 207, 208, 209, 216, and 217, for the open Internet rules we adopt today to address practices that are unjust, unreasonable, or unreasonably discriminatory."); *see also* para. 25 ("Reclassification will enhance the Commission's ability to ensure Internet openness, defend national security, promote cybersecurity, safeguard public safety, monitor network resiliency and reliability, protect consumer privacy and data security, support consumer access to BIAS, and improve disability access.").

[185] *2024 Open Internet Order* at paras. 28-29.

[186] 47 U.S.C. § 201(b); *see also* 47 U.S.C. § 202.

[187] 47 U.S.C. § 201.

[188] *See* CSRIC III, Working Group 6 - Secure BGP Deployment Final Report at 20 (2013), http://www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_SocialMediaUsers.pdfhttps://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_%202013.pdf (explaining that widespread RPKI implementation could make the Internet routing system more secure by providing accurate information about which ASes are authorized to originate routes for each IP prefix).

[189] *See, e.g.,* 47 U.S.C. §§ 303, 307, 309, 316.

[190] 47 U.S.C. § 303(b).

[191] 47 U.S.C. § 1302.

[192] 47 U.S.C. § 1302(b).

[193] 47 U.S.C. § 1302(d)(1).

to remove barriers to infrastructure investment.[194] We believe that our proposed measures would facilitate infrastructure investment by promoting secure and reliable Internet infrastructure, thereby facilitating the widespread availability of advanced telecommunications capability to all Americans.

102. Additionally, we tentatively conclude that the Communications for Law Enforcement Act (CALEA) also grants authority to the Commission to secure Internet routing. Section 105 of CALEA provides that "[a] telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission."[195] The Commission has explained that this provision requires telecommunications carriers to secure their networks against unauthorized interception of communications.[196] We tentatively conclude that CALEA authorizes the Commission to impose RPKI security requirements on facilities-based service providers because doing so would help prevent the unlawful interception of communications. A router's advertisement of intentionally incorrect routing information can cause an unauthorized interception of communications that, we tentatively conclude, CALEA section 105 requires carriers to prevent. The objective of preventing illegal interception is in harmony with what the Commission is trying to achieve in this proceeding and, more broadly, reflects an intent by Congress that the Commission maintain an active role in adopting and enforcing safeguards that protect the security of communications networks where the public interest so requires. We seek comment on whether CALEA gives the Commission authority to require RPKI measures as part of its duty to "prescribe such rules as are necessary to implement the requirements of [CALEA]."[197]

103. We seek comment on these observations and any other views on potential sources of authority for our proposed Internet routing safeguards.

### G. Promoting Digital Equity

104. The Commission, as part of its continuing effort to advance digital equity for all, including people of color, persons with disabilities, persons who live in rural or Tribal areas, and others who are or have been historically underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related considerations, and invites comment on any benefits (if any) that may be associated with the proposals and issues discussed herein.[198] Specifically, we seek

[194] 47 U.S.C. § 1302(a).

[195] 47 U.S.C. § 1004. The U.S. Court of Appeals for D.C. Circuit has upheld the Commission's decision that CALEA applies to facilities-based broadband Internet access service providers. *American Council on Educ. v. FCC*, 451 F.3d 226 (D.C. Cir. 2006) (affirming *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, RM-10865, First Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 14989 (2005)).

[196] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11436-37, paras. 35-37.

[197] 47 U.S.C. § 229(a).

[198] Section 1 of the Communications Act of 1934 as amended provides that the FCC "regulat[es] interstate and foreign commerce in communication by wire and radio so as to make [such service] available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex." 47 U.S.C. § 151. The term "equity" is used here consistent with Executive Order 13985 as the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality. *See* Exec. Order No. 13985, 86 Fed.

(continued….)

comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well as the scope of the Commission's relevant legal authority.

## IV. PROCEDURAL MATTERS

105. *Paperwork Reduction Act.* This document contains proposed new and modified information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.[199]

106. *Providing Accountability Through Transparency Act*. Consistent with the Providing Accountability Through Transparency Act, Public Law 118-9, a summary of this document will be available on https://www.fcc.gov/proposed-rulemakings.

107. *Ex Parte Rules*. This proceeding shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules, with a limited exception described in the following paragraph.[200] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with Rule 1.1206(b). In proceedings governed by Rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

108. In order to facilitate the free exchange of exploratory ideas among the staff of the federal agencies working toward the critical goal of promoting secure Internet routing, and in light of the secure Internet routing Initiatives as part of the National Cybersecurity Strategy, we find the public interest requires a limited modification of the *ex parte* status in this proceeding.[201] Communications between the Commission staff and staff of the Federal Government entities with a formal role in these Internet security matters, i.e., ONCD, CISA, DOJ, Office of the Director of National Intelligence, and NTIA shall be exempt from the rules requiring disclosure in permit-but-disclose proceedings and exempt from the

Reg. 7009, Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (Jan. 20, 2021).

[199] *See* 44 U.S.C. § 3506(c)(4).

[200] 47 CFR §§ 1.1200, 1.1206.

[201] 47 CFR § 1.1200(a) ("Where the public interest so requires in a particular proceeding, the Commission and its staff retain the discretion to modify the applicable ex parte rules by order, letter, or public notice."); *see also Biden NCSIP*, Initiative Number 4.1.5, at 38; *Biden NCS* at 23-24.

prohibitions during the Sunshine Agenda period.[202] To be clear, while the Commission recognizes that consultation with these entities is critically important, the Commission will rely in its decision-making only on facts and arguments that are placed in the public record for this proceeding. To this end, the enumerated Federal Government entities, like all interested parties, should submit in the public record of this proceeding comments, reply comments, and other presentations presenting those facts and arguments they wish the Commission to rely on in its decision-making process.[203]

109. *Regulatory Flexibility Act*. The Regulatory Flexibility Act of 1980, as amended (RFA), requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities." [204] Accordingly, the Commission has prepared an Initial Regulatory Flexibility Analysis concerning the possible impact of the rule and policy changes contained in this *Notice of Proposed Rulemaking*. The IRFA is set forth in Appendix B. Written public comments are requested on the IRFA. Comments must be filed by the deadlines for comments on the Notice indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA.

110. *Confidentiality*. We recognize that some comments could contain information that the submitter believes should not be made available to the general public because of commercial or national security reasons. Parties may request that such information be kept confidential, identifying the specific information sought to be kept confidential, providing the reasons for the request, and otherwise following the procedures set forth in section 0.459 of our rules.[205] If a party requests confidential treatment of a comment, it must file an original and one copy of the confidential version of the comment on paper, following the procedures below, and a public version of the filing that omits only the confidential information and is otherwise identical to the confidential version, using either the electronic filing or the filing-by-paper procedures below.[206] The redacted document must be machine-readable whenever technically possible.[207] If the document to be filed electronically contains confidential metadata or is otherwise protected from disclosure by a legal privilege (e.g., attorney-client privilege), such metadata may be removed from the document before the filer submits it electronically.[208]

111. *Filing Requirements—Comments and Replies*. Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: https://www.fcc.gov/ecfs/.

[202] *See generally* 47 CFR § 1.1206; *id.* § 1.1203.

[203] If the presentation made by staff of one of the federal agencies enumerated above is of "substantial significance and clearly intended to affect the ultimate decision," the Commission will rely on such presented information in its decision-making process only if it coordinates in advance with the agency involved to ensure that such agency retains control over the timing and extent of any disclosure that may impact that agency's jurisdictional responsibilities. *See* 47 CFR § 1.1206(b)(3).

[204] *See* 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601–612, was amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[205] 47 CFR § 0.459.

[206] 47 CFR § 1.1206(b)(2)(ii).

[207] *Id.*

[208] *Id.*

- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.
- Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
    - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
    - Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street, NE, Washington, DC 20554.
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19.[209]
- During the time the Commission's building is closed to the general public and until further notice, if more than one docket or rulemaking number appears in the caption of a proceeding, paper filers need not submit two additional copies for each additional docket or rulemaking number; an original and one copy are sufficient.

112. *People with Disabilities*. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an email to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice).

113. *Additional Information*. For further information regarding the Notice, please contact George Donato, Associate Division Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-0729, or by email to george.donato@fcc.gov; or James Zigouris, Attorney-Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-0697, or by email to james.zigouris@fcc.gov.

## V. ORDERING CLAUSES

114. Accordingly, IT IS ORDERED that pursuant to sections 1, 2, 3, 4, 10, 201, 202, 208, 209, 214, 216, 217, 218, 219, 220(a), 229, 251, 254, 255, 256, 301, 303, 307, 332, and 333, of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 153, 154(i)-(j), 160, 201, 202, 208, 209, 214, 216, 217, 218, 219, 220(a), 229, 251, 254, 255, 256, 301, 303, 332, 333 that this *Notice of Proposed Rulemaking* IS hereby ADOPTED.

115. IT IS FURTHER ORDERED that the Commission's Office of the Secretary, SHALL SEND a copy of this *Notice of Proposed Rulemaking*, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

Marlene H. Dortch
Secretary

[209] *See FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy*, Public Notice, 35 FCC Rcd 2788 (2020).

## APPENDIX A

### Technical Appendix: Additional Background on Inter-Domain Routing

1. Information traverses the Internet in the data fields of Internet protocol (IP) packets. Each version of IP (of which there are currently two established standards, IPv4 and IPv6) specifies the most fundamental formats and semantics of Internet data transfer. Every IP packet includes a source and destination address, to indicate the source and destination of that IP packet, representing the corresponding endpoints. These networked endpoints may communicate through a medium access layer mechanism if the communicating endpoints are on a local area / non-routed network. Alternatively, when the networked endpoints are on separate networks, the endpoints communicate via IP routers that compile reachability data using routing protocols. In any sizable collection of networked endpoints, for reasons of resilient design and network management, individual Local Area Network segments are connected by IP routers that support one or more routing protocols.

2. Routing protocols implement the signaling mechanisms that exchange reachability information between or within independent networks, as to destinations available and the network paths by which to reach them. There are specialized categories of routing protocols for signaling, depending on whether the routing protocols are deployed within independent networks (Interior Gateway Protocols or IGPs) or between independently managed networks (External Gateway Protocols or EGPs). Each category of routing protocol has different performance characteristics and functional optimizations. Of the two major candidate protocols, Inter Domain Routing Protocol and the Border Gateway Protocol (BGP), that were considered for use as EGPs, BGP emerged as the ubiquitous deployment choice. As mentioned earlier, the Internet consists of approximately 70,000 independently administered and managed networks at the time of writing. [1] These networks use BGP to signal reachability information to reflect both technical priorities and business objectives, in terms of permitting a choice of the next hop of the path to carry their external traffic. In this way, BGP is termed as a "path vector" routing protocol.[2] However, since BGP also supports business priorities by allowing path selection, BGP is also said to support policy-based routing.[3]

3. The networks interconnected by BGP are termed BGP Autonomous Systems (ASes) and are referred to by their Autonomous System Numbers (ASNs).[4] An AS may include one or multiple separate networks, collectively all under the technical administration of a single entity. For BGP purposes, a network path is denoted as a string of ASNs termed an AS Path. The AS Path is one of the "BGP path attributes" or control variables used in signaling BGP reachability that influences how each BGP speaker selects routes to a specific destination. Originally, the AS Path was intended to reflect the initial ASN originating an advertisement for a prefix, as well as the succession of ASes traversed by a BGP update (the basic BGP message carrying signaling information).[5] However, no means were provided to verify whether this attribute was correct or false in any way. Deliberations on how best to

[1] *See supra* para. 6.

[2] Cisco Press, *It's Time to Hang Up on Robocalls for Good* (Jan. 1, 2018), https://www.ciscopress.com/articles/article.asp?p=2756480.

[3] Juniper Networks, *Understanding BGP Path Selection* (Dec. 12, 2023), https://www.juniper.net/documentation/us/en/software/junos/vpn-l2/bgp/topics/concept/routing-protocols-address-representation.html(*Understanding BGP Path Selection*).

[4] Cloudflare, *What is an autonomous system?*, https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/ (last visited Apr. 3, 2024).

[5] *Understanding BGP Path Selection*.

address this type of risk and others have occurred since at least 1997.[6] As these and other references cited note, there are additional vulnerabilities that go beyond the ones described in this section.

4. A BGP route can be defined as a destination prefix associated with a string of BGP Path attributes. Attributes provide the semantics that affect how the BGP logic in each BGP speaker processes the routes it receives from other BGP speakers. The BGP hijacks referred to in this item deal with incidents associated with manipulating the AS Path attribute, including distorting or falsifying the Origin AS, or the originated route specificity. Some of the relatively more well-known routing incidents have involved these attack vectors.[7]

5. Internet addressing conventions have implications for BGP routing, since BGP routers advertise the reachability of destination addresses to which they can find a path. Reachability information exchange occurs by exchanging BGP protocol data units or packets that contain the necessary information using the formats and semantics specified in BGP standard documents.[8] To allow BGP routing to scale, Internet Service Providers (ISPs) are required to aggregate the IP address space in the route advertisements they originate into a compacted contiguous block that forms the "network prefix." Doing so reduces the number of route table entries needed to cover the full scope of available Internet destinations, thus diminishing the size of the routing table in those routers central to routing topology in the so-called "default-free zone." Since memory and route look up speeds both affect router operation, this form of aggregation allows the number of addressable endpoints to grow and the Internet to scale while still retaining acceptable performance in the routers that carry the most comprehensive sets of routes, in effect constituting a connectivity core for the Internet. However, a route that is more specific than one that is aggregated is preferred by the BGP state machine, so announcing this will preferentially attract traffic relative to a route advertising an aggregate. This attack vector is somewhat distinct from AS PATH manipulation and has been used in prior BGP hijack incidents as well.[9]

6. Details of the concepts introduced above are further explained in several accessible reference works, including the primer entitled "Security of the Internet's Routing Infrastructure," issued by the Broadband Internet Technical Advisory Group (BITAG).[10] For more information beyond the summary descriptions in this section, readers are referred to the text on "Network Routing" in the Morgan Kaufman series in Networking or, for simplified review, the BITAG document as well as the OECD publication on routing security.[11]

[6] *See* B. R. Smith and J. J. Garcia-Luna-Aceves, *Securing the Border Gateway Routing Protocol*, Proceedings of GLOBECOM'96. 1996 IEEE Global Telecommunications Conference at 81-85 (1996); *see also* IETF, RFC 4272 - BGP Security Vulnerabilities Analysis at 6 (2006), https://www.rfc-editor.org/rfc/rfc4272; and IETF, RFC 7132 - Threat Model for BGP Path Security at 2 (2014), https://www.rfc-editor.org/rfc/rfc7132.

[7] Doug Madory, *A Brief History of the Internet's Biggest BGP Incidents* (June 6, 2023), https://www.kentik.com/blog/a-brief-history-of-the-internets-biggest-bgp-incidents/(*A Brief History*).

[8] Juniper Networks, *Supported Standards for BGP* (Jan. 22, 2024), https://www.juniper.net/documentation/us/en/software/junos/standards/bgp/topics/concept/bgp.html.

[9] *A Brief History*.

[10] BITAG, Security of the Internet's Routing Infrastructure at 6-8 (2022), https://www.bitag.org/documents/BITAG_Routing_Security.pdf.

[11] Deep Medhi & Karthik Ramasamy, Network Routing: Algorithms, Protocols, and Architectures (2d ed. 2017).

## APPENDIX B

### Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Federal Communications Commission (Commission) has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the Notice of Proposed Rulemaking (*Notice*). Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments specified on the first page of the *Notice*. The Commission will send a copy of the *Notice*, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[2] In addition, the *Notice* and IRFA (or summaries thereof) will be published in the Federal Register.[3]

### A. Need for, and Objectives of, the Proposed Rules

1. In the *Notice*, the Commission proposes measures for securing Internet routing to improve public safety in view of vulnerabilities that threaten the security and integrity of the Border Gateway Protocol (BGP). BGP is a routing protocol which is central to the Internet's global routing system because it allows the exchange of information amongst independently managed networks on the Internet. During this exchange of information, packets of data are routed along advertised paths provided by these independent networks to reach their intended destination. However, routing incidents can occur which result in the data not arriving at the intended destination because of misdirection, interception, and/or manipulation caused by the actions of a bad actor. These routing incidents—whether intentional or accidental—can affect the functioning and quality of service of the Internet because they can disrupt the flow of Internet traffic.

2. The proposals in the *Notice* are part of ongoing multi-stakeholder efforts to address secure Internet routing issues. President Biden's National Cybersecurity Strategy, which highlights the critical nature of securing the technical foundation of the Internet, expressly identifies addressing BGP vulnerabilities as one of the most urgent actions necessary to further this objective.[4] Significantly, Initiative 4.1.5 of the National Cybersecurity Strategy Implementation Plan tasks the Office of the National Cyber Director (ONCD), working with key stakeholders and other Federal Government entities, to develop a roadmap to increase adoption of secure Internet routing techniques, including those that address BGP security concerns.[5]

3. In the *Notice*, the Commission seeks comment on proposed measures to address BGP vulnerabilities which would be applicable to providers of broadband Internet access service (BIAS), including comments on the proposed measures for Route Origin Validation (ROV). These measures include requiring providers of BIAS on a mass market retail basis (service providers) to prepare and

[1] 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601 – 612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] 5 U.S.C. § 603(a).

[3] *Id*.

[4] Executive Office of the President, National Cybersecurity Strategy at 23-24 (2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[5] Initiative 4.1.5, Collaborate with key stakeholders to drive secure Internet routing, *National Cybersecurity Strategy Implementation Plan,* https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf (last visited Apr. 14, 2024).

annually file confidential BGP Routing Security Risk Management Plans (BGP Plans) describing and attesting to the specific efforts they have made, and plan to undertake, to secure their Internet routing architecture using Resource Public Key Infrastructure (RPKI), and to include information on Route Origin Authorization (ROA) registrations and maintenance for their route originations, and their Route Origin Validation (ROV) status and deployment plans. The proposed measures also include only requiring certain identified providers that are able to reach all Internet endpoints solely through peering relationships and other significant providers to file BGP Plans with the Commission while all other providers would be required to maintain and make their plans available upon Commission request. Similarly, quarterly filings of specific data would only be required by the identified providers that are able to reach all Internet endpoints solely through peering relationships and other significant providers.

4. Building on this proposed RPKI measure, the Commission also seeks comment on what, if anything, service providers can or should do to help secure ROA for the IP address space held by downstream or peering entities. Finally, we invite comments on whether we should require measures for securing a route's pathway as well, and we seek comment on which techniques and architecture should be proposed to secure the route's pathway. Additionally, recognizing the importance of increased outreach and education about the security risks of BGP, and of the role that the American Registry for Internet Numbers (ARIN) (the Regional Internet Registry) and its processes play in the deployment of more secure RPKI routing, the Commission seeks comment on the steps we should take participate in those efforts.

### B. Legal Basis

5. The proposed action is authorized pursuant to sections 1, 2, 3, 4, 10, 201, 202, 208, 209, 214, 216, 217, 218, 219, 220(a), 229, 251, 254, 255, 256, 301, 303, 307, 332, and 333, of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 153, 154(i)-(j), 160, 201, 202, 208, 209, 214, 216, 217, 218, 219, 220(a), 229, 251, 254, 255, 256, 301, 303, 307, 332, and 333.

### C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

6. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the proposed rules and policies, if adopted.[6] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[7] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[8] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[9]

7. *Small Businesses, Small Organizations, and Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein.[10] First, while there are industry specific size standards for small businesses that are used in the regulatory

[6] 5 U.S.C. § 603(b)(3).

[7] 5 U.S.C. § 601(6).

[8] 5 U.S.C. § 601(3)(incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[9] 15 U.S.C. § 632.

[10] *See* 5 U.S.C. § 601(3)-(6).

flexibility analysis, according to data from the SBA Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[11] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 33.2 million businesses.[12]

8. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[13] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[14] Nationwide, for tax year 2022, there were approximately 530,109 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[15]

9. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[16] U.S. Census Bureau data from the 2022 Census of Governments[17] indicate there were 90,837 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number, there were 36,845 general purpose governments (county, municipal, and town or township) with populations of less than 50,000 and 11,879 special purpose governments (independent school districts) with enrollment

[11] *See* SBA, Office of Advocacy, "What's New With Small Business?," https://advocacy.sba.gov/wp-content/uploads/2023/03/Whats-New-Infographic-March-2023-508c.pdf (Mar. 2023).

[12] *Id*.

[13] 5 U.S.C. § 601(4).

[14] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number of small organizations in this small entity description. S*ee* Annual Electronic Filing Requirement for Small Exempt Organizations – Form 990-N (e-Postcard), "Who must file," https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[15] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for businesses for the tax year 2022 with revenue less than or equal to $50,000 for Region 1-Northeast Area (71,897), Region 2-Mid-Atlantic and Great Lakes Areas (197,296), and Region 3-Gulf Coast and Pacific Coast Areas (260,447) that includes the continental United States, Alaska, and Hawaii. This data includes information for Puerto Rico (469).

[16] 5 U.S.C. § 601(5).

[17] 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/economic-census/year/2022/about.html. *See* U.S. Census Bureau, 2022 Census of Governments – Organization Table 2. Local Governments by Type and State: 2022 [CG2200ORG02], https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* tbl.2. CG2200ORG02 Table Notes_Local Governments by Type and State_2022.

populations of less than 50,000.[18] Accordingly, based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 entities fall into the category of "small governmental jurisdictions."[19]

### 1. Internet Access Service Providers

10. *Wired Broadband Internet Access Service Providers (Wired ISPs)*.[20] Providers of wired broadband Internet access service include various types of providers except dial-up Internet access providers. Wireline service that terminates at an end user location or mobile device and enables the end user to receive information from and/or send information to the Internet at information transfer rates exceeding 200 kilobits per second (kbps) in at least one direction is classified as a broadband connection under the Commission's rules.[21] Wired broadband Internet services fall in the Wired Telecommunications Carriers industry.[22] The SBA small business size standard for this industry classifies firms having 1,500 or fewer employees as small.[23] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[24] Of this number, 2,964 firms operated with fewer than 250 employees.[25]

11. Additionally, according to Commission data on Internet access services as of June 30, 2019, nationwide there were approximately 2,747 providers of connections over 200 kbps in at least one

[18] *See id.* at tbl.5. County Governments by Population-Size Group and State: 2022 [CG2200ORG05], https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html. There were 2,097 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments. *See id.* at tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2022 [CG2200ORG06], https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html. There were 18,693 municipal and 16,055 town and township governments with populations less than 50,000. On special purpose governments, *see id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2022 [CG2200ORG10], https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html. There were 11,879 independent school districts with enrollment populations less than 50,000. *See also* tbl.4. Special-Purpose Local Governments by State Census Years 1942 to 2022 [CG2200ORG04], CG2200ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2022. While the special purpose governments category also includes local special district governments, the 2022 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[19] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,845) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (11,879), from the 2022 Census of Governments - Organizations tbls. 5, 6 & 10.

[20] Formerly included in the scope of the Internet Service Providers (Broadband), Wired Telecommunications Carriers, and All Other Telecommunications small entity industry descriptions.

[21] *See* 47 CFR § 1.7001(a)(1).

[22] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[23] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[24] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[25] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

direction using various wireline technologies.[26] The Commission does not collect data on the number of employees for providers of these services, therefore, at this time we are not able to estimate the number of providers that would qualify as small under the SBA's small business size standard. However, in light of the general data on fixed technology service providers in the Commission's *2022 Communications Marketplace Report*,[27] we believe that the majority of wireline Internet access service providers can be considered small entities.

12. *Wireless Broadband Internet Access Service Providers (Wireless ISPs or WISPs)*.[28] Providers of wireless broadband Internet access service include fixed and mobile wireless providers. The Commission defines a WISP as "[a] company that provides end users with wireless access to the Internet[.]"[29] Wireless service that terminates at an end user location or mobile device and enables the end user to receive information from and/or send information to the Internet at information transfer rates exceeding 200 kilobits per second (kbps) in at least one direction is classified as a broadband connection under the Commission's rules.[30] Neither the SBA nor the Commission have developed a size standard specifically applicable to WISPSs. The closest applicable industry with an SBA small business size standard is Wireless Telecommunications Carriers (except Satellite).[31] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[32] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[33] Of that number, 2,837 firms employed fewer than 250 employees.[34]

13. Additionally, according to Commission data on Internet access services as of June 30, 2019, nationwide there were approximately 1,237 fixed wireless and 70 mobile wireless providers of connections over 200 kbps in at least one direction.[35] The Commission does not collect data on the number of employees for providers of these services, therefore, at this time we are not able to estimate the

[26] *See* Federal Communications Commission (FCC), Internet Access Services: Status as of June 30, 2019 at 27, Fig. 30 *(IAS Status 2019)*, Industry Analysis Division, Office of Economics & Analytics (March 2022). The report can be accessed at https://www.fcc.gov/economics-analytics/industry-analysis-division/iad-data-statistical-reports. The technologies used by providers include aDSL, sDSL, Other Wireline, Cable Modem, and FTTP). Other wireline includes: all copper-wire based technologies other than xDSL (such as Ethernet over copper, T-1/DS-1, and T3/DS-1), as well as power line technologies which are included in this category to maintain the confidentiality of the providers.

[27] *See Communications Marketplace Report*, GN Docket No. 22-203, 2022 WL 18110553 at 10, paras. 26-27, Figs. II.A.5-7 (2022)(*2022 Communications Marketplace Report*).

[28] Formerly included in the scope of the Internet Service Providers (Broadband), Wireless Telecommunications Carriers (except Satellite), and All Other Telecommunications small entity industry descriptions.

[29] Federal Communications Commission, Internet Access Services: Status as of June 30, 2019 at 27, Fig. 30 *(IAS Status 2019)*, Industry Analysis Division, Office of Economics & Analytics (March 2022). The report can be accessed at https://www.fcc.gov/economics-analytics/industry-analysis-division/iad-data-statistical-reports.

[30] *See* 47 CFR § 1.7001(a)(1).

[31] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[32] *See* 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[33] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[34] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[35] *See IAS Status 2019,* Fig. 30.

number of providers that would qualify as small under the SBA's small business size standard. However, based on data in the Commission's *2022* Communications *Marketplace Report* on the small number of large mobile wireless nationwide and regional facilities-based providers, the dozens of small regional facilities-based providers and the number of wireless mobile virtual network providers in general, as well as on terrestrial fixed wireless broadband providers in general,[36] we believe that the majority of wireless Internet access service providers can be considered small entities.

14. *Broadband Personal Communications Service*. The broadband personal communications services (PCS) spectrum encompasses services in the 1850-1910 and 1930-1990 MHz bands.[37] The closest industry with an SBA small business size standard applicable to these services is Wireless Telecommunications Carriers (except Satellite).[38] The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[39] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[40] Of this number, 2,837 firms employed fewer than 250 employees.[41] Thus under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

15. Based on Commission data as of November 2021, there were approximately 5,060 active licenses in the Broadband PCS service.[42] The Commission's small business size standards with respect to Broadband PCS involve eligibility for bidding credits and installment payments in the auction of licenses for these services. In auctions for these licenses, the Commission defined "small business" as an entity that, together with its affiliates and controlling interests, has average gross revenues not exceeding $40 million for the preceding three years, and a "very small business" as an entity that, together with its affiliates and controlling interests, has had average annual gross revenues not exceeding $15 million for the preceding three years.[43] Winning bidders claiming small business credits won Broadband PCS licenses in C, D, E, and F Blocks.[44]

16. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect

[36] *See 2022 Communications Marketplace Report*, 2022 WL 18110553 at 27, paras. 64-68; at 8, para. 22.

[37] *See* 47 CFR § 24.200.

[38] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[39] *See* 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[40] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[41] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[42] Based on a FCC Universal Licensing System search on November 16, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = CW; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[43] *See* 47 CFR § 24.720(b).

[44] *See* FCC, Office of Economics and Analytics, Auctions, Auctions 4, 5, 10, 11, 22, 35, 58, 71 and 78, https://www.fcc.gov/auctions.

data on the number of employees for licensees providing these, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

17. *Broadband Radio Service and Educational* Broadband Service. Broadband Radio Service systems, previously referred to as Multipoint Distribution Service (MDS) and Multichannel Multipoint Distribution Service (MMDS) systems, and "wireless cable,"[45] transmit video programming to subscribers and provide two-way high speed data operations using the microwave frequencies of the Broadband Radio Service (BRS) and Educational Broadband Service (EBS) (previously referred to as the Instructional Television Fixed Service (ITFS)).46 Wireless cable operators that use spectrum in the BRS often supplemented with leased channels from the EBS, provide a competitive alternative to wired cable and other multichannel video programming distributors. Wireless cable programming to subscribers resembles cable television, but instead of coaxial cable, wireless cable uses microwave channels.[47]

18. In light of the use of wireless frequencies by BRS and EBS services, the closest industry with an SBA small business size standard applicable to these services is Wireless Telecommunications Carriers (*except* Satellite).[48] The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[49] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[50] Of this number, 2,837 firms employed fewer than 250 employees.[51] Thus under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

19. According to Commission data as December 2021, there were approximately 5,869 active BRS and EBS licenses.[52] The Commission's small business size standards with respect to BRS involves eligibility for bidding credits and installment payments in the auction of licenses for these services. For the auction of BRS licenses, the Commission adopted criteria for three groups of small businesses. A

[45] The use of the term "wireless cable" does not imply that it constitutes cable television for statutory or regulatory purposes.

[46] *See* 47 CFR § 27.4; *see also Amendment of Parts 21 and 74 of the Commission's Rules with Regard to Filing Procedures in the Multipoint Distribution Service and in the Instructional Television Fixed Service and Implementation of Section 309(j) of the Communications Act—Competitive Bidding*, Report and Order, 10 FCC Rcd 9589, 9593, para. 7 (1995).

[47] Generally, a wireless cable system may be described as a microwave station transmitting on a combination of BRS and EBS channels to numerous receivers with antennas, such as single-family residences, apartment complexes, hotels, educational institutions, business entities and governmental offices. The range of the transmission depends upon the transmitter power, the type of receiving antenna and the existence of a line-of-sight path between the transmitter or signal booster and the receiving antenna.

[48] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[49] *See* 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[50] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[51] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[52] Based on a FCC Universal Licensing System search on December 10, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service =BR, ED; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

very small business is an entity that, together with its affiliates and controlling interests, has average annual gross revenues that exceed $3 million and did not exceed $15 million for the preceding three years, a small business is an entity that, together with its affiliates and controlling interests, has average gross revenues that exceed $15 million and did not exceed $40 million for the preceding three years, and an entrepreneur is an entity that, together with its affiliates and controlling interests, has average gross revenues not exceeding $3 million for the preceding three years.[53] Of the ten winning bidders for BRS licenses, two bidders claiming the small business status won four licenses, one bidder claiming the very small business status won three licenses, and two bidders claiming entrepreneur status won six licenses.[54] One of the winning bidders claiming a small business status classification in the BRS license auction has an active license as of December 2021.[55]

20. The Commission's small business size standards for EBS define a small business as an entity that, together with its affiliates, its controlling interests, and the affiliates of its controlling interests, has average gross revenues that are not more than $55 million for the preceding five (5) years, and a very small business is an entity that, together with its affiliates, its controlling interests, and the affiliates of its controlling interests, has average gross revenues that are not more than $20 million for the preceding five (5) years.[56] In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

21. *Internet Service Providers (Non-Broadband)*. Internet access service providers using client-supplied telecommunications connections (e.g., dial-up ISPs) as well as VoIP service providers using client-supplied telecommunications connections fall in the industry classification of All Other Telecommunications.[57] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[58] For this industry, U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[59] Of those firms, 1,039

[53] *See* 47 CFR § 27.1218(a).

[54] *See* Federal Communications Commission, Economics and Analytics, Auctions, Auction 86: Broadband Radio Service, Summary, Reports, All Bidders, https://www.fcc.gov/sites/default/files/wireless/auctions/86/charts/86bidder.xls.

[55] Based on a FCC Universal Licensing System search on December 10, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service =BR; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[56] *See* 47 CFR § 27.1219(a).

[57] *See* U.S. Census Bureau, *2017 NAICS Definition, "517919 All Other Telecommunications*," https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[58] *See* 13 CFR § 121.201, NAICS Code 517919 (as of 10/1/22, NAICS Code 517810).

[59] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

had revenue of less than $25 million.[60] Consequently, under the SBA size standard a majority of firms in this industry can be considered small.

### 2. Satellite Service Providers

22. *Satellite Telecommunications*. This industry comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[61] Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $38.5 million or less in annual receipts as small.[62] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[63] Of this number, 242 firms had revenue of less than $25 million.[64] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 65 providers that reported they were engaged in the provision of satellite telecommunications services.[65] Of these providers, the Commission estimates that approximately 42 providers have 1,500 or fewer employees.[66] Consequently, using the SBA's small business size standard, a little more than half of these providers can be considered small entities.

23. *All Other Telecommunications*. This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[67] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[68] Providers of Internet services (e.g. dial-up ISPs) or VoIP services, via client-supplied telecommunications connections are also included in this industry.[69] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[70] U.S.

[60] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* U.S. Census Bureau, *Glossary*, https://www.census.gov/glossary/#term_ReceiptsRevenueServices (last visited May 14, 2024).

[61] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications*,*"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[62] *See* 13 CFR § 121.201, NAICS Code 517410.

[63] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[64] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* U.S. Census Bureau, *Glossary*, https://www.census.gov/glossary/#term_ReceiptsRevenueServices (last visited May 14, 2024).

[65] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[66] *Id.*

[67] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications*," https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[68] *Id.*

[69] *Id*.

[70] *See* 13 CFR § 121.201, NAICS Code 517919 (as of 10/1/22, NAICS Code 517810).

Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[71] Of those firms, 1,039 had revenue of less than $25 million.[72] Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

### 3. Other Providers

24. *All Other Information Services*. This industry comprises establishments primarily engaged in providing other information services (except news syndicates, libraries, archives, Internet publishing and broadcasting, and Web search portals).[73] The SBA small business size standard for this industry classifies firms with annual receipts of $30 million or less as small.[74] U.S. Census Bureau data for 2017 show that there were 704 firms in this industry that operated for the entire year.[75] Of those firms, 556 had revenue of less than $25 million.[76] Consequently, we estimate that the majority of firms in this industry are small entities.

## D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

25. The proposed measures for service providers outlined in this *Notice* are to increase public safety by addressing vulnerabilities in Internet routing. The Commission expects the proposed measures in the *Notice*, if adopted, will may impose new reporting, recordkeeping, notice or other compliance requirements on small entities that act as service providers to provide Internet service and/or Internet access. These requirements may include application or other conformance reporting, licensing, certification and/or other reporting obligations.

26. Small and other service providers that provide service on a mass market retail basis would be required to prepare and update confidential BGP Plans at least once per year. The BGP Plan reporting requirement would require ISPs to describe and attest to the specific efforts they have made, and plan to undertake, to secure their Internet routing architecture using RPKI as well as other methods at their disposal (e.g., peer-locking). The BGP Plan would also require ISPs to include, among other things, the ISPs' plans for ROA registrations and maintenance for their route originations, and the status of and plans for their deployment of ROV. The Commission's proposed filing requirements include requiring a select

[71] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[72] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[73] *See* U.S. Census Bureau, *2017 NAICS Definition, "519190 All Other Information Services,"* https://www.census.gov/naics/?input=519190&year=2017&details=519190.

[74] *See* 13 CFR § 121.201, NAICS Code 519190 (as of 10/1/22, NAICS Codes 519290).

[75] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEREVFIRM, NAICS Code 519190, https://data.census.gov/cedsci/table?y=2017&n=519190&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[76] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We note that the U.S. Census Bureau withheld publication of the number of firms that operated with sales/value of shipments/revenue of less than $100,000 to avoid disclosing data for individual companies (see Cell Notes for the sales/value of shipments/revenue in this category). Therefore, the number of firms revenue that meet the SBA size standard would be higher than noted herein. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* U.S. Census Bureau, *Glossary*, https://www.census.gov/glossary/#term_ReceiptsRevenueServices (last visited May 14, 2024).

number of the largest ISPs to file their BGP Plans with the Commission annually, while small and other remaining service providers would only be required to maintain and make their BGP Plans available to Commission staff upon request. The Commission also proposes to require larger ISPs to file quarterly reports containing select data points to measure progress in RPKI deployment and assess whether reporting on additional measures may be needed.

27. The proposals in the *Notice* build upon other actions the Commission has taken to protect and secure public safety. The Commission notes that the proposals being made in this *Notice* may require additional analysis and mitigation activities by small and other ISPs to satisfy certain technical criteria or standards for the ability to address Internet routing vulnerabilities. At this time, the Commission is not in a position to determine whether the proposals that may be adopted for ISPs would require small entities to hire professionals in order to comply and cannot quantify the cost of compliance with the potential requirements and obligations that may result in this proceeding. Among other things considered, we inquire about the options for the Commission to address the costs of adopting the proposed measures for ROV. We seek comment on these issues and anticipate that the information we receive in comments will address these matters and any broader cost issues for small entities that may be affected by the proposed measures.

28. We expect that the comments we receive will help the Commission identify and evaluate relevant matters for small entities before adopting final rules for securing Internet routing, including any compliance costs and burdens that may result from the proposals and other matters discussed in the *Notice*.

### E. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

29. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[77]

30. The proposals in the *Notice* to secure Internet routing build on the work of the Communications Security, Reliability, and Interoperability Councils (CSRICs), federal advisory committees made up of telecommunications industry stakeholders as well as special advisors from other relevant sectors to address issues associated with the security of communications systems, and particularly on the work products of CSRIC III and CSRIC VI, for securing Internet routing. Using the work of CSRIC III and CSRIC VI as a foundation has the potential to minimize the economic impact on small entities for several reasons. First, CSRIC III took into account existing best practices for securing Internet routing.[78] Next, CSRIC VI recommended best practices established by the Mutually Agreed Norms for Routing Security (MANRS) and the Internet Engineering Task Force (IETF).[79] The Commission believes building on these widely accepted measures would only require minimal adjustments for small and other ISPs to comply with the proposals for securing Internet routing in the

[77] 5 U.S.C. § 603(c).

[78] *See* CSRIC III, Secure BGP Deployment, Final Report at 11-12 (2013), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_%202013.pdf.

[79] CSRIC VI, Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols, Final Report at 4-15, 6-20 (2019), https://www.fcc.gov/sites/default/files/csric6wg3_finalreport_030819.pdf.

*Notice* and would provide a level of consistency among ISPs which all play a part in routing Internet traffic.

31. The Commission recognizes that smaller service providers may have relatively fewer in-house resources available than larger Tier 1 providers to secure Internet routing, and therefore has taken specific steps to minimize the obligations bore by small providers. For example, the Commission does not propose a one-size fits all approach to address BGP vulnerabilities with a set of industry-wide requirements and deadlines. The flexible approach the Commission proposes still expects smaller providers to meet requirements to secure Internet routing, however, as an alternative to the proposed requirement that ISPs file BGP Plans with the Commission, as mentioned above, the Commission proposes that smaller service providers prepare, update, and maintain BGP Plans, and make such plans available within 48 hours of a Commission request. The Commission also proposes significantly limited data reporting requirements in the BGP Plans for small providers and proposes that only larger carriers as defined in the Notice be required to file quarterly data reports.

32. In the *Notice*, the Commission considers and seeks comment on various measures for validating route origin during Internet routing including ROV filtering. We include a requirement that all BGP Plans describe the contractual requirements the service provider has for upstream third parties to provide ROV filtering for their Internet traffic. Tier 3 service providers who are typically small providers, and do not have peering relationships and only rely on upstream contracts with other service providers, would not need to file this information with the Commission but alternatively would be required to have the information available upon Commission request. Additionally, small providers that are classified as Tier 2 providers and have peering relationships with other Tier 2 providers, or contractual relationships with Tier 1 providers, would benefit from the Commission's proposal to allow Tier 2 providers two years to implement the requirement to support ROV for both directly connected peers with settlement-free access as well as their directly connected clients, including other service providers, rather than the one year implementation deadline for required for Tier 1 providers.

33. The Commission expects to consider the economic impact and alternatives more fully for small entities following the review of comments filed in response to the *Notice.* Having input from interested parties will allow the Commission to better evaluate options and alternatives to minimize any significant economic impact on small entities that may result from implementing the proposed measures discussed in the *Notice*. The Commission's evaluation of this information will shape the final alternatives it considers to minimize any significant economic impact that may occur on small entities, the final conclusions it reaches and any final rules it promulgates in this proceeding.

### F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

34. None.