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

In the Matter of	)	
	)	
Secure Internet Routing	)	PS Docket No. 22-90
	)	

NOTICE OF INQUIRY

Adopted: February 28, 2022 **Released: February 28, 2022**

Comment Date: 30 days after Federal Register Publication
Reply Comment Date: 60 days after Federal Register Publication

By the Commission:

I. INTRODUCTION

1. The Commission plays an important role in protecting the security of America's communications networks and critical infrastructure. The Commission, in tandem with its federal partners, has urged the communications sector to defend against cyber threats, while also taking measures to reinforce our Nation's readiness and to strengthen the cybersecurity of vital communications services and infrastructure, especially in light of Russia's escalating actions inside of Ukraine. Today, we build on those efforts. With this *Notice of Inquiry* (*Notice*), we seek comment on vulnerabilities threatening the security and integrity of the Border Gateway Protocol (BGP), which is central to the Internet's global routing system, its impact on the transmission of data from email, e-commerce, and bank transactions to interconnected Voice-over Internet Protocol (VoIP) and 9-1-1 calls, and how best to address them.

2. BGP is the routing protocol used to exchange reachability information amongst independently managed networks on the Internet.[1] BGP's initial design, which remains widely deployed today, does not include security features to ensure trust in the information that it is used to exchange.[2] As a result, a bad network actor may deliberately falsify BGP reachability information to redirect traffic to itself or through a specific third-party network, and prevent that traffic from reaching its intended

[1] *See* BGP Best Path Selection Algorithm, CISCO Doc ID 13753 (Sept. 12, 2016), https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html. These independently managed networks (also termed "domains") loosely map to one or more "Autonomous Systems" (so termed because the administration of the network is the sole responsibility of a single, independent entity). *See* ARIN, *Requesting IP Addresses or ASNs*, https://www.arin.net/resources/guide/request/ (last visited Feb. 23, 2022).

[2] *See* The Internet Society, A Border Gateway Protocol 4 (BGP-4) (2006), https://datatracker.ietf.org/doc/html/rfc4271. BGP was designed at a time when the number of independently managed networks on the Internet was low and the trust among them was high.

recipient.[3] These "BGP hijacks" expose U.S. citizens' personally identifiable information, enable theft, extortion, and state-level espionage, and disrupt otherwise-secure transactions.[4]

II. BACKGROUND

3. Congress created the Commission, among other reasons, "for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communications."[5] To obtain "maximum effectiveness from the use of radio and wire communications in connection with the safety of life and property," the Communications Act of 1934, as amended, directs the Commission to "investigate and study all phases of the problem and the best methods of obtaining the cooperation and coordination" of such systems."[6]

4. The Commission has taken targeted steps to protect the nation's communications infrastructure from potential security threats.[7] Most recently, the Commission encouraged communications companies to review cybersecurity practices to defend against threats to critical infrastructure,[8] sought comment on how the Commission can leverage its equipment authorization program to encourage device manufacturers to consider cybersecurity standards and guidelines,[9] and

[3] *See Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*, NIST Spec. Pub. 800-189, at 3 (2019), https://csrc.nist.gov/publications/detail/sp/800-189/final; *see also* Internet Society, *MANRS Mutually Agreed Norms for Routing Security*, https://www.internetsociety.org/issues/manrs/ (last visited Feb. 23, 2022) (citing thousands of incidents of misrouted traffic or denial of service each year). When a bad actor directs traffic to be dropped in this way, it is commonly referred to as a "blackhole." *See*, *e.g.*, *YouTube and Pakistan Telecom*, https://youtu.be/IzLPKuAOe50 (last visited Feb. 23, 2022).

[4] *See Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation*, NIST Spec. Pub. 1800-14, at 6 (2019), https://csrc.nist.gov/publications/detail/sp/1800-14/final. We use the term "BGP hijacking" to refer to any deliberate injection of routing information away from the optimal (or most secure) route, including both false route origination and path interception attacks.

[5] 47 U.S.C. § 151.

[6] 47 U.S.C. § 154(n).

[7] *See*, *e.g.*, *China Mobile International (USA) Inc.; Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended*, Memorandum Opinion and Order, 34 FCC Rcd 3361 (2019) (*China Mobile USA Denial Order*); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs et al.*, WC Docket No. 18-89 et al., Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423 (2019); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, 35 FCC Rcd 7821, 7822, paras. 2-3 (2020); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284, 14285, para. 1 (2020); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Third Report and Order, FCC 21-86 (July 14, 2021); *China Telecom (Americas) Corporation*, GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, Order on Revocation and Termination, FCC 21-114 (Nov. 2, 2021) (*China Telecom Americas Order on Revocation and Termination*); *China Unicom (Americas) Limited*, GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427, Order on Revocation, FCC 22-9 (Feb. 2, 2022) (*China Unicom Americas Order on Revocation*).

[8] *See FCC Urges Communications Companies to Review Cybersecurity Practices to Defend Against Cyber Threats to Critical Infrastructure*, Public Notice, DA 22-75 (PSHSB Jan. 21, 2022).

[9] *See Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*; *Protecting Against National Security threats to the Communications Supply Chain through the Competitive Bidding Program*, ET Docket No. 21-232, EA Docket No. 21-233, Notice of Proposed Rulemaking and Notice of Inquiry, FCC 21-73, paras. 98-105 (June 17, 2021).

acted in the public interest to deny and revoke the section 214 authority of certain carriers to provide telecommunications service in the United States.[10]

5. Independently managed networks are essential to the daily functioning of critical infrastructure such as transportation, gas and electric power, water, and financial markets.[11] These networks can be vulnerable to attack if they deploy a version of BGP at their borders that cannot verify the integrity or authenticity of routing information.[12] BGP's vulnerabilities allow a network operator to accidentally or maliciously misconfigure its BGP routers to falsely advertise that its network contains the intended destination for certain Internet traffic, or is on the path to that destination. By advertising incorrect routing information, a bad actor could spread incorrect information to other networks and cause traffic intended for the advertised destination to be misrouted to, or through, the bad actor's network. Causing Internet traffic to depart from its most efficient path is termed "BGP hijacking."[13] Although BGP hijacking can occur anywhere on the global Internet, the Commission has an interest in minimizing or eliminating opportunities for it within its jurisdiction because it can potentially harm U.S. citizens, commerce, and public safety operations.

6. Russian network operators have been suspected of exploiting BGP's vulnerability to hijacking, including instances in which traffic has been redirected through Russia without explanation.[14] In late 2017, for example, traffic sent to and from Google, Facebook, Apple and Microsoft was briefly routed through an Internet service provider in Russia.[15] That same year, traffic from a number of financial institutions, including MasterCard, Visa, and others was also routed through a Russian government-controlled telecommunications company under "unexplained" circumstances.[16]

7. Over the past two decades, Internet stakeholders have developed new standards, specifications, and best practice recommendations intended to address the security risk that BGP poses.[17] The Internet Engineering Task Force (IETF), the principal authority responsible for Internet standards, has finalized several standards to reduce BGP vulnerabilities, including BGPsec, an extension to BGP that provides security for the path through which reachability information passes.[18] The National Institute

---

[10] *See generally China Mobile USA Denial Order; China Telecom Americas Order on Revocation and Termination* (revoking and terminating China Mobile's section 214 authority); *China Unicom Americas Order on Revocation*.

[11] Border routers are also referred to as "edge routers." *See* Cloudflare, *What is BGP?*, https://www.cloudflare.com/learning/security/glossary/what-is-bgp/ (last visited Feb. 23, 2022).

[12] These vulnerabilities have two main causes: (1) validating a route's origin; and (2) securing and validating the correct BGP path to a given destination.

[13] *See Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*, NIST Spec. Pub. 800-189, Sec. 2.1 (2019), https://csrc.nist.gov/publications/detail/sp/800-189/final; Kevin Butler et al., *A Survey of BGP Security Issues and Solutions*, 98 Proceedings of the IEEE 1, at 100-122 (Jan. 2010), https://www.cise.ufl.edu/~butler/pubs/bgpsurvey.pdf.

[14] *See*, *e.g.*, Dan Goodin, *Repeated attacks hijack huge chunks of Internet traffic, researchers warn* (Nov. 20, 2013), https://arstechnica.com/information-technology/2013/11/repeated-attacks-hijack-huge-chunks-of-internet-traffic-researchers-warn/.

[15] *See* Dan Goodin, *"Suspicious" event routes traffic for big-name sites through Russia* (Dec. 13, 2017), https://arstechnica.com/information-technology/2017/12/suspicious-event-routes-traffic-for-big-name-sites-through-russia/.

[16] *See* Dan Goodin, *Russian-controlled telecom hijacks financial services' Internet traffic* (Apr. 7, 2017), https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/.

[17] *See* Douglas Montgomery, *Towards Secure Routing Infrastructures*, 4 IEEE Security & Privacy 5 (Jan. 2006) https://www.nist.gov/publications/toward-secure-routing-infrastructures.

[18] *See* IETF, *Secure Inter-Domain Routing*, https://datatracker.ietf.org/wg/sidr/documents/ (last visited Feb. 23, 2022); IETF, BGPsec Protocol Specification (2017), https://www.rfc-editor.org/rfc/pdfrfc/rfc8205.txt.pdf.

of Standards and Technology (NIST) has released a practice guide proposing a method of validating routes' origins and recommendations for resilient exchange between independently managed networks.[19] In 2017, the Internet Society launched Mutually Agreed Norms for Routing Security (MANRS),[20] an organizational initiative with membership including over 700 network operators, Internet Service Providers, and enterprises, which aims to reduce or prevent route hijacking and denial of service attacks by requiring network operators to implement available tools and applicable IETF Best Common Practice standards.[21] MANRS offers a tool called "MANRS Observatory" that aggregates data from trusted sources into a dashboard to help network operators improve the security of their networks.[22] Similarly, the Commission's Communications Security, Reliability, and Interoperability Council (CSRIC) has reported on best practices and recommendations to improve the security of BGP.[23] CSRIC III recommended that network operators ensure that BGP routers' Internet routing registries are accurate, complete, and up-to-date, and that network operators use a standards-based approach for providing cryptographically secure registries of Internet resources and routing authorizations, a Resource Public Key Infrastructure (RPKI).[24] CSRIC VI recommended that network operators support MANRS and IETF Best Common Practice standards.[25] Notwithstanding this work, available information suggests that the voluntary adoption and deployment of such measures has been such that many of the independently

[19] *See Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation*, NIST Spec. Pub. 1800-14 (2019), https://csrc.nist.gov/publications/detail/sp/1800-14/final; *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*, NIST Spec. Pub. 800-189 (2019), https://csrc.nist.gov/publications/detail/sp/800-189/final; Oliver Borchert, et al., BGP Secure Routing Extension (BGP-SRx): Reference Implementation and Test Tools for Emerging BGP Security Standards, White Paper NIST Technical Note (TN) 2060 (2021), https://csrc.nist.gov/publications/detail/white-paper/2021/09/15/bgp-secure-routing-extension-bgp-srx/final.

[20] *See Mutually Agreed Norms for Routing Security (MANRS)*, https://www.manrs.org/ (last visited Feb. 23, 2022). MANRS focuses on improving routing security by filtering routing advertisements to include only those likely to be relevant to the customer BGP router; enabling source IP address validation for customer networks; coordinating and sharing contact information for network operations center contacts through regional Internet registries, and enabling routing information to be validated on a global scale.

[21] *See*, *e.g.*, The Internet Society, Network Ingress Filtering Defeating Denial of Service Attacks which Employ IP Source Address Spoofing (2000), https://www.rfc-editor.org/rfc/pdfrfc/rfc2827.txt.pdf; The Internet Society, Recommended Internet Service Provider Security Services and Procedures (2000), https://www.rfc-editor.org/rfc/pdfrfc/rfc3013.txt.pdf; The IETF Trust, Current Operational Security practices in Internet Service Provider Environments (2007), https://datatracker.ietf.org/doc/html/rfc4778.

[22] *See* MANRS, Observatory, https://observatory.manrs.org/#/overview (last visited Feb. 23, 2022).

[23] *See* CSRIC III, Secure BGP Deployment, Final Report (2013), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_%202013.pdf; CSRIC VI, Report on best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols, Final Report (2019), https://www.fcc.gov/file/15311/download. The roman numerals following the name of federal advisory committee, "CSRIC," enumerate the successive years during which the Commission has chartered CSRIC to provide recommendations on selected topics.

[24] In this connection, the FCC sought comment on the implementation and effectiveness of the CSRIC III recommendations and/or alternatives that stakeholders have developed since the time of the CSRIC's original work to address these challenges. *See 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).

[25] *See* CSRIC VI, Report on best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols, Final Report, at 20-21 (2019), https://www.fcc.gov/file/15311/download.

managed networks that comprise the Internet remain vulnerable because they have not taken advantage of these measures.[26]

III. DISCUSSION

8. *Scope of Inquiry.* In this *Notice*, we seek comment on any steps that the Commission should consider taking to help protect and strengthen the nation's communications network and other critical infrastructure from vulnerabilities posed by BGP, and how we can best facilitate the implementation of industry standards and best practices to mitigate the potential harms posed by these vulnerabilities. In order to better understand the BGP ecosystem, we seek comment on the extent to which Internet Service Providers, public Internet Exchange Providers, and providers of interconnected VoIP service have deployed BGP routers in their networks. Do content delivery networks, and providers of cloud services operate BGP routers in their networks as well? What other types of entities operate BGP routers? We recognize that there are entities that do not operate BGP routers, but that are otherwise well positioned to support the development and implementation of BGP security practices. For example, there are several regional, national, and local Internet registries that manage the allocation and registration of Internet number resources, and support RPKIs.[27] Additionally, the Internet Corporation for Assigned Names and Numbers (ICANN), through its affiliate, Internet Assigned Numbers Authority (IANA), has responsibility for coordinating the Internet's unique identifiers. We seek comment on what role these and other entities, including vendors of BGP routers or other networking equipment, have in supporting the development and implementation of BGP security practices. What threats to Internet routing should the Commission consider within the scope of this inquiry in addition to BGP hijacking? For example, to what extent could BGP security measures prevent pervasive monitoring?[28]

9. *Measuring BGP Security.* We seek comment on whether industry has defined metrics for identifying BGP routing security incidents and for quantifying their scope and impact. To what extent are available tools, such as NIST's RPKI Monitor, Automatic and Real-Time dEtection and Mitigation System (ARTEMIS), BGPstream, BGPMon, Kentik, and Traceroute, able to rapidly and accurately detect BGP hijacks or router misconfigurations?[29] To what extent do these tools distinguish malicious routing changes from accidental ones? Do artificial intelligence and machine learning tools promise advancements in this area?

10. *Deployment of BGP Security Measures.* We seek comment on the security measures that have been developed and deployed by industry to secure BGP. In addition to the measures recommended by CSRIC III and VI (RPKI, MANRS, and applicable IETF Best Common Practice standards), BGPsec,

---

[26] *Compare* The 32-bit AS Number Report, https://www.potaroo.net/tools/asn32/ (counting 72,635 independently managed networks on the Internet as of February 16, 2022) *with* MANRS Steering Committee Needs You, https://www.manrs.org/2021/09/the-manrs-steering-committee-needs-you/ (last visited Feb. 21, 2022) (stating that over 700 entities participate in MANRS representing over 750 autonomous systems); *see also* MANRS Observatory, https://observatory.manrs.org/#/overview (last visited Feb. 23, 2022).

[27] As an example, one such regional Internet registry, the American Registry for Internet Numbers (ARIN) supports the roles of a digital certificate authority and acts as a repository for routing information and as a validator of RPKI data. *See* ARIN, Resource Certification, https://www.arin.net/resources/manage/rpki/ (last visited Feb. 23, 2022).

[28] *See* IETF, Pervasive Monitoring is an Attack (2014), https://datatracker.ietf.org/doc/html/rfc7258.

[29] *See NIST RPKI Monitor*, https://rpki-monitor.antd.nist.gov/ (last visited Feb. 23, 2022); *RIPE Labs, ARTEMIS: An Open-source Tool for Detecting BGP Prefix Hijacking in Real Time* (Aug. 21, 2017), https://labs.ripe.net/author/vasileios_kotronis/artemis-an-open-source-tool-for-detecting-bgp-prefix-hijacking-in-real-time/; Cisco, *BGPstream*, https://bgpstream.com/ (last visited Feb. 23, 2022); Cisco, *BGPMon*, https://bgpmon.net/ (last visited Feb. 23, 2022); *Kentik*, https://www.kentik.com/ (last visited Feb 23, 2022); KC Claffy, Border Gateway Protocol (BGP) and Traceroute Data Workshop Report and Traceroute Data Workshop Report, https://www.caida.org/catalog/papers/2012_bgp_traceroute_report/bgp-traceroute_report.pdf; Tamir Carmeli, Detection of BGP Hijacking Using TTL Analysis (2018), https://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2018/MSC/MSC-2018-05.pdf.

and the NIST practice guide, what other standards, specifications, or best practices have been developed to address potential attacks that exploit BGP vulnerabilities? We seek comment on the extent to which network operators have implemented any of the available BGP security measures developed by industry. How effective are these measures in practice? We seek comment on how to assess, measure, demonstrate, or increase the effectiveness of these security measures. To the extent that network operators have not implemented security measures, we seek comment on why such measures have not been implemented. To the extent that network operators have implemented security measures, how effective have they been at mitigating the vulnerability? What obstacles have prevented them from doing so?

11. We seek comment on the extent to which RPKI, as implemented by other regional Internet registries, effectively prevents BGP hijacking. To what extent do network operators take advantage of the RPKI services that regional Internet registries offer by implementing RPKI in their networks?[30] To what extent, if any, do network operators' service level agreements affect the ability of network operators to drop traffic that RPKI deems invalid? How do regional Internet registries maintain the certificate authority for the RPKIs in a way that mitigates the risk of a single point of failure vulnerable to distributed denial of service attacks? How do regional Internet registries prevent conflicts among distributed RPKI trust anchors?

12. We seek comment on whether and to what extent network operators anticipate integrating BGPsec-capable routers into their networks. The specification for the BGPsec extension to BGP became available in 2017, but it appears that BGPsec has not been widely deployed despite BGP's known vulnerabilities.[31] Why have network operators not taken more aggressive steps to adopt BGPsec? What particular obstacles or concerns about BGPsec have slowed their adoption? To what extent does the introduction of BGPsec routers potentially introduce compatibility issues among managed networks or introduce delays? [32]

13. For network operators that currently participate in MANRS and comply with its requirements, including support for IETF Best Common Practice standards, we seek comment on the efficacy of such measures for preventing BGP hijacking.[33] To what extent do the network operators that participate in MANRS support both its required and recommended routing security actions,[34] as well as applicable IETF Best Common Practice standards on which those actions are based? To what extent do network operators participate in MANRS' various programs, including its equipment vendor program,

---

[30] *See* NIST, *RPKI Monitor*, https://rpki-monitor.antd.nist.gov/ (last visited Feb. 22, 2022) (showing that 34% of IPv4 Internet traffic is validated using RPKI).

[31] *See* Phillip Smith, BGP Origin Validation, ISP Workshops (2022), https://bgp4all.com/pfs/_media/workshops/02-rpki.pdf; *see also* BGPsec, *History*, https://bgpsec.net/history.html (last visited Feb. 24, 2022) (targeting 2026 for a global launch of BGPsec).

[32] *See* Robert Lychev, et al., BGP Security in Partial Deployment (2013), https://www.cs.bu.edu/~goldbe/papers/partialSec.pdf (purporting to show that partial deployment of BGPsec performs poorly, can cause instability, and is susceptible to downgrade attacks).

[33] *See* MANRS, MANRS Community Report 2021 (2022), https://www.manrs.org/resources/community-report-2021/; MANRS, MANRS Community Report 2020 (2021), https://www.manrs.org/resources/community-report-2020/ ("The number of reported routing incidents has been decreasing from more than 5,000 in 2017 to below 4,000 at the end of 2020, while the number of MANRS participants has been increasing"); Hosting Journalist, *All China Telecom Backbone Networks Now Meeting MANRS Security Standards* (Jun. 6, 2021), https://hostingjournalist.com/all-china-telecom-backbone-networks-now-meeting-manrs-security-standards/.

[34] *See MANRS for Network Operators*, v. 2.5.2 (May 17, 2021). https://www.manrs.org/isps/; *MANRS for IXPs*, https://www.manrs.org/ixps/ (last visited Feb. 16, 2021); *MANRS for CDN and Cloud Providers*, https://www.manrs.org/cdn-cloud-providers/ (last visited Feb. 16, 2021); *MANRS for Equipment Vendors*, https://www.manrs.org/equipment-vendors/ (last visited Feb. 16, 2021).

launched in 2021, which aims to enable routing security features on network equipment and provide support and training guidance to use them, or take advantage of the MANRS Observatory.[35]

14. *Commission's Role.* Ensuring continued U.S. leadership requires that we explore opportunities to spur trustworthy innovation for more secure communications and critical infrastructure. The Commission has sought to promote the security of U.S. networks and network equipment both by drawing attention to available resources and through exercise of its regulatory authority.[36] We seek comment on steps the Commission, in coordination with other federal agencies,[37] could take to prevent BGP hijacking or otherwise promote secure Internet routing. We seek comment on whether the Commission has a role in helping U.S. network operators deploy BGP security measures. If so, how can the Commission be most helpful? We seek comment on our authority to promote the security of Internet routing through regulation, including as it may apply to wireless and wireline Internet Service Providers, Internet Exchange Providers, interconnected VoIP providers, operators of content delivery networks, cloud service providers, and other enterprise and organizational stakeholders. We seek comment on whether regulatory clarity could help network operators prioritize investments in the security of their networks.

15. We seek comment on the extent to which other nations' telecommunications regulators and multistakeholder organizations have issued rules, guidance, or otherwise encouraged network operators, network security organizations, and equipment vendors to implement BGP security measures and on any lessons learned from those endeavors. We seek comment on the extent to which the effectiveness of BGP security measures may be related to international participation and coordination.

16. *Costs and Benefits.* We seek comment on the one-time and ongoing costs of implementing the BGP security measures discussed herein. What capital and operational expenditures attend their implementation? Does the availability of a protocol for RPKI keep implementation costs low? Would network operators need to replace existing routers to support the BGPsec extension? Could support be enabled through a software upgrade, particularly for routers that are not considered to be "end-of-life"? To what extent can network operators support MANRS' required and recommended actions by updating their policies and practices, and without equipment replacement or software updates? What costs would consumer likely experience from BGP security implementations, such as higher service costs or speed reductions?

17. We seek comment on whether the Commission should encourage industry to prioritize the deployment of BGP security measures within the networks on which critical infrastructure and emergency services rely, as a means of helping industry to control costs otherwise associated with a network-wide deployment. Would this or another phased or gradual implementation of BGP security measures be effective and help network operators to plan for and control implementation costs?

18. We also seek comment on the national security, economic, and public safety benefits of more secure Internet routing, both within the U.S. and globally. What entities are particularly affected by

[35] *See* Converge, *Leading vendors agree to tackle vulnerabilities in global routing* (Sep. 15, 2021), https://www.convergedigest.com/2021/09/leading-vendors-agree-to-tackle.html (stating that this initiative is backed by Arista, Cisco, Huawei, Juniper, and Nokia).

[36] *See*, *e.g.*, *FCC Urges Communications Companies to Review Cybersecurity Practices to Defend Against Cyber Threats to Critical Infrastructure*, Public Notice, DA 22-75 (PSHSB Jan. 21, 2022); *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*; *Protecting Against National Security threats to the Communications Supply Chain through the Competitive Bidding Program*, ET Docket No 21-232, EA Docket No. 21-233, Notice of Proposed Rulemaking and Notice of Inquiry, FCC 21-73, paras. 98-105 (Jun. 17, 2021); *China Telecom (Americas) Corporation*, GN Docket No. 20-109, ITC-214-20010613-00346; ITC-214-20020716-00371; ITC-T/C-20070725-00285, Order on Revocation and Termination, FCC 21-114, para. 2 (Nov. 2, 2021).

[37] Other federal agencies are engaged in cybersecurity and specifically BGP security, including NIST, the Department of Homeland Security, and the National Telecommunications and Information Administration.

threats to BGP security? To what extent would the security measures discussed herein be effective in mitigating BGP hijacking? What is the potential impact of mitigating BGP hijacking on U.S. national security and the U.S. economy? Have stakeholders attempted to quantify the benefits that secure Internet routing could convey by protecting critical infrastructure, sensitive communications, and personally identifiable information? Have stakeholders attempted to quantify the benefits of secure Internet routing in terms of the potential loss of Intellectual Property, communications delays, or disruptions that BGP's unmitigated vulnerability represents? Have stakeholders attempted to measure or quantify the extent to which BGP hijacking poses a threat to life and property by disrupting 9-1-1 calls carried by providers of interconnected VoIP service? What other benefits could potentially accrue from this inquiry?

19. *Digital Equity and Inclusion.* Finally, the Commission, as part of its continuing effort to advance digital equity for all,[38] 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[39] and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well the scope of the Commission's relevant legal authority.

IV. PROCEDURAL MATTERS

20. *Ex Parte Rules*. This proceeding shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[40] 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), 47 CFR § 1.1206(b). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

---

[38] 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.

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

[40] 47 CFR § 1.1200(a). Although the rules do not generally require *ex parte* presentations to be treated as "permit but disclose" in Notice of Inquiry proceedings, *see* 47 CFR § 1.1204(b)(1), we exercise our discretion in this instance, and find that the public interest is served by making *ex parte* presentations available to the public, in order to encourage a robust record. *See id.* § 1.1200(a).

21. *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.[41] 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.

22. *Comment Filing Procedures* 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) or by paper. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

- Electronic Filers: Comments may be filed electronically by accessing ECFS at https://www.fcc.gov/ecfs.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing. Paper filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail.
    - 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.[42]
    - 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.
    - U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE, Washington, D.C. 20554.

23. *Availability of Documents*. Comments, reply comments, and *ex parte* submissions will be publicly available online via ECFS. These documents will also be available for public inspection during regular business hours in the FCC Reference Information Center, when FCC Headquarters reopen to the public.

24. *People with Disabilities*. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

25. *Further Information*. For additional information on this proceeding, contact James Wiley of the Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, at james.wiley@fcc.gov or (202) 418-1678 or Minsoo Kim of the Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, at minsoo.kim@fcc.gov or (202) 418-1739.

V. ORDERING CLAUSES

26. Accordingly, IT IS ORDERED, pursuant to sections 1, 4(i)-(j), 4(n), 7, and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154(i)-(j), 154(n), 157 and Section 1.430 of the Commission's rules, 47 CFR § 1.430, that this NOTICE OF INQUIRY IS ADOPTED.

---

[41] 47 CFR § 0.459.

[42] *See* FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, 35 FCC Rcd 2788 (2020), https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary