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

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

REPLY COMMENTS OF FASTLY

David Sando
Vice President & Deputy General Counsel

Job Snijders
Principal Engineer

Fastly, Inc.
475 Brannan Street, Suite 300
San Francisco, CA 94017
www.fastly.com

May 10, 2022

Table of Contents

I. INTRODUCTION AND SUMMARY

Fastly, Inc. ("Fastly") appreciates the opportunity to respond to comments on the Federal Communication Commission's ("FCC" or "Commission") Notice of Inquiry ("NOI") regarding the Border Gateway Protocol ("BGP"), and to add its unique perspective to the record in this proceeding.[1] Fastly shares the Commission's goal of "protecting the security of America's communications networks;"[2] indeed, this is an important goal for the global Internet. Fastly's edge cloud platform is built around security and performance. As an edge cloud platform provider, Fastly is well-positioned to provide insight into Internet routing.

Fastly is committed to fostering innovation and empowering developers to create modern digital experiences. Fastly supports and is a key part of the global Internet ecosystem. Fastly technical experts serve on a variety of Internet engineering and governance bodies, including the Internet Engineering Task Force ("IETF") Global Routing Operations (grow) working group.[3]

This NOI seeks comment on "vulnerabilities threatening the security and integrity of the Border Gateway Protocol (BGP), which is central to the Internet's global routing system."[4] Of particular interest to Fastly, the NOI asks about Content Delivery Networks ("CDN") and cloud

---

[1] *Secure Internet Routing*, Notice of Inquiry, FCC 22-18, PS Docket No. 22-90 (Mar. 11, 2022), https://www.federalregister.gov/documents/2022/03/11/2022-05121/secure-internet-routing ("NOI").

[2] *Id.* ¶ 1.

[3] IETF, *Global Routing Operations (grow)*, https://datatracker.ietf.org/group/grow/about/ (last visited May 9, 2022).

[4] NOI ¶ 1.

providers operating BGP routers in their networks,[5] the effectiveness and deployment of security measures,[6] and the economic benefits of more secure routing.[7]

With these reply comments, Fastly seeks to clarify some key points raised by the commenters so far, and to emphasize to the Commission that routing is integral to the operations of edge cloud, traditional CDN, and cloud providers. Fastly strongly supports implementing secure routing, and is among the many Internet stakeholders working diligently to devise and implement technology and process solutions to the issues raised in the NOI (among many others). Secure routing technology is steadily advancing through innovation and implementation of new technologies, but given the scale of the Internet and the scope of the issues that need to be addressed, no single solution will be completely effective—it will take a range of tools and services to meet these challenges. Moreover, although technologies like BGPsec can be updated today on modern hardware, not all existing systems can support its demands. The natural pace of hardware and software development means that these systems will eventually be upgraded (and BGPsec's computational efficiency will likely increase), but it will likely be years before technologies like BGPsec can be fully implemented. Thus, while Fastly applauds the FCC for drawing attention to this issue, and encourages the Commission to support secure routing technology adoption, it would be premature for any regulator to attempt to impose mandates for particular technological solutions.

[5] *Id.* ¶ 8.

[6] *Id.* ¶ 8, 9.

[7] *Id.* ¶ 18.

II. FASTLY SUPPORTS AND IMPLEMENTS SECURITY AND RELIABILITY ACROSS ITS PLATFORM.

A. Routing is at the Heart of Fastly's Business.

Fastly is an edge cloud provider that provides reliable, scalable, and secure digital experiences. Fastly's edge cloud platform is a CDN of the type mentioned in the NOI;[8] it makes transmission of content more efficient by placing points of presence ("POPs") where connectivity to the Internet reduces transit time. Each POP is a cluster of Fastly cache servers, and when an end user requests content objects from a Fastly customer, Fastly delivers them from whichever cache locations are closest to that end user.[9]

Fastly offers a wide variety of capabilities for web applications and developers that ensure the speed and reliability of web traffic. Fastly takes a software-centric approach to drive network efficiency and flexibility. Its routing capabilities enable solutions such as traffic distribution, traffic management, live streaming at scale, and responsive mobile applications.

Fastly's software and infrastructure thus sit between its customers and their end users, offering Fastly a unique perspective on the need for secure routing, and the various challenges that network providers face in building and implementing routing solutions. Indeed, helping to facilitate secure routing is at the core of the services that Fastly provides.

B. Fastly Devotes Significant Time and Attention to Global Internet Community Stewardship.

As the Commission notes in the NOI, the Internet community works through a collaborative, multi-stakeholder process to develop new standards, specifications, and best

[8] *Id.* ¶ 8.

[9] For more information on Fastly's service, please see Fastly, *How Fastly's CDN Service works* (last updated Sept. 9, 2021), https://docs.fastly.com/en/guides/how-fastlys-cdn-service-works.

practices recommendations for secure routing.[10] Fastly technical experts serve on a variety of Internet engineering and governance bodies and have devoted their time and expertise to IETF matters including QUIC,[11] RSA-BSSA,[12] HTTP prioritization,[13] BGP4,[14] and RPKI.[15] These groups do critical work and play a central role in addressing this global challenge.

III. FASTLY CONCURS WITH PROMOTING ADOPTION OF SECURE ROUTING.

A. Global Adoption is a Massive, Decades-Long Project.

As several commenters explained, the Internet is vast in scale, comprising today over 70,000 individual Autonomous Systems ("AS"), each corresponding to an organization such as an Internet Service Provider, cloud provider, CDN, or university.[16] The owners of ASes differ in size, sophistication, capability, purpose, and location. BGP is a foundational tool for allowing the Internet to function, as it establishes the standard by which these diverse ASes communicate routing information amongst one another.[17]

The number and diversity of actors on the Internet is a daunting reality. Stakeholders are working continuously through Internet governance bodies and standards organizations to develop

---

[10] *See* NOI ¶ 7.

[11] IETF, *QUIC (quic)*, https://datatracker.ietf.org/wg/quic/about/ (last visited May 9, 2022).

[12] IETF, *Crypto Forum (cfrg)*, https://datatracker.ietf.org/rg/cfrg/about/ (last visited May 9, 2022).

[13] IETF, *HTTP Working Group*, https://httpwg.org/ (last visited May 9, 2022).

[14] IETF, *Inter-Domain Routing (idr)*, https://datatracker.ietf.org/wg/idr/about/ (last visited May 9, 2022).

[15] IETF, *SIDR Operations (sidrops)*, https://datatracker.ietf.org/wg/sidrops/about/ (last visited May 9, 2022).

[16] *See generally* Comments of David Clark, KC Claffy, and Cecilia Testart, PS Docket No. 22-90, at 1, 3 (filed Apr. 11, 2022) ("Clark Comments").

[17] Comments of Juniper Networks, PS Docket No. 22-90, at 3 (filed Apr. 1, 2022) ("Juniper Comments").

and define ways to secure Internet routing, and major providers that route a large portion of the world's traffic can make a significant difference by adopting secure routing practices. Nevertheless, the scale of the undertaking means that this is a decades-long process. It is not something that can simply be implemented overnight.

B. While the Timeframes for Adoption Are Significant, Substantial Progress is Being Made.

The Internet and its diverse stakeholders are not standing still on this important issue. The Commission should take notice of the evolution of routing security approaches over the past two decades. Cryptographic verification was introduced as RFC 3779 in 2004, the foundational RFC that relied on X509 certificates.[18] As early as 2006, experts identified a roadmap for development that was prescient and still relevant over fifteen years later.[19] That a fifteen-year-old report is still relevant is not evidence of lack of progress, but rather a testament to the scope of the project of moving the entire Internet from a plaintext routing system to an encrypted one.

Fastly concurs with the commenters who point to the Resource Public Key Infrastructure ("RPKI") as an important framework for building routing security.[20] The implementation of Route Origin Validation ("ROV") through RFC 6811,[21] based on this RPKI framework, is just the first step in implementing a diversified means of addressing routing security issues. The next generation of secure routing will be built around integrating cryptographic verification. Fastly and

---

[18] IETF, *X.509 Extensions for IP Addresses and AS Identifiers* (June 2004), https://datatracker.ietf.org/doc/html/rfc3779.

[19] Sparta, Inc., Secure Protocols for the Routing Infrastructure (SPRI) Initiative: A Road Map (First Draft) (Sept. 2006), https://www.bgpsec.net/dhs_roadmap_for_fixing_internet_protocols.pdf.

[20] *See, e.g.*, Comments of Cloudflare, PS Docket No. 22-90, at 7-8 (filed Apr. 11, 2022) ("Cloudflare Comments").

[21] IETF, *BGP Prefix Origin Validation* (Jan. 2013), https://datatracker.ietf.org/doc/rfc6811/.

others have worked to develop**,** study**,** and implement BGPsec, which when widely adopted will be another major step in promoting security. As many have noted, because BGPsec is far more involved than ROV, it requires vastly more computational power.[22]

However, Fastly disagrees with those commenters who see BGPsec as unlikely to achieve widespread adoption.[23] While BGPsec implementation has challenges, the barriers to full-scale adoption relate to computational demand on existing hardware—and these barriers will fall over time. *First*, BGPsec itself will continue to evolve, in ways that are likely to reduce the demand that it places on the hardware running it, as computational optimization for BGPsec implementation continues. BGPsec is a "versioned" application and the protocol has and will continue to evolve. The next evolution of BGPsec is expected to be available in three to five years and is likely to afford significant speed increases, and further improvement can be expected as development continues.

Second, widespread BGPsec deployment will become easier as the industry's overall hardware upgrade cycle continues. BGPsec can run today on modern hardware, but the machines that can handle the cryptographic tasks necessary to implement BGPsec are not yet ubiquitously deployed. This will not be true forever—routing hardware is subject to finite life-cycles, and as older hardware is replaced across the world with newer, more capable gear, the costs imposed by BGPsec implementation will naturally decrease.

Thus, while it would be inaccurate to say that BGPsec is fully mature and ready for widespread adoption today, it is also wrong to assume that broad adoption of BGPsec will never occur. The software and hardware enhancements that will allow widespread BGPsec deployment

[22] Juniper Comments at 6.

[23] Internet Society, Ex Parte Filing, PS Docket No. 22-90, at 1 (filed Mar. 29, 2022).

are not speculative; they are part of the routine lifecycle of research, development, and capital investment by a range of Internet stakeholders. Over the next decade or so, BGPsec will likely be integrated by the Internet community into routing across the world.

Moreover, BGPsec is not the only new tool in development for improving routing security. For example, global stakeholders are also developing Autonomous System Provider Authorization ("ASPA") on a separate development track from BGPsec. As explained in more detail below, ASPA is not a substitute for BGPsec, but will instead provide complementary protection for Internet routing.[24] And while ASPA is behind BGPsec in terms of development and standard setting, its implementation requires less computational power and may be easier and quicker than BGPsec deployment.

Improvements in routing security need not rely solely on the deployment of new tools. There are several existing best practices that can be adopted with additional awareness and training for network operators and administrators.[25] These practices have been developed over the years through diligent effort by stakeholders, and would substantially enhance security now if they were more widely adopted. For example, network operators should establish required default policies for BGP speakers under RFC 8212,[26] and set maximum prefix limits.[27] The Internet community

[24] IETF, *A Profile for Autonomous System Provider Authorization* (working draft) (Jan. 31, 2022), https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-profile/ ("IETF ASPA working draft").

[25] *See generally* Netherlands Network Operators' Group, *BGP Filter Guide*, https://bgpfilterguide.nlnog.net/ (last visited May 9, 2022).

[26] IETF, *Default External BGP (EBGP) Route Propagation Behavior without Policies* (July 2017), https://datatracker.ietf.org/doc/html/rfc8212.

[27] National Security Agency, A Guide to Border Gateway Protocol (BGP) Best Practices, at 10 (Sept. 10, 2018), https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/ctr-guide-to-border-gateway-protocol-best-practices.pdf?v=1.

has twenty years of experience in developing and testing these practices, but the population of experts in routing configuration and cryptographic key management is small. Groups like the North American Network Operators' Group ("NANOG") provide critical training and professional development that can dramatically increase global capability, but require additional support and awareness from network operators to scale their impact. The Commission should work with Internet stakeholders and other U.S. government agencies to highlight these best practices and to encourage their more widespread use.

C. The Commission Should Gather More Data.

Additional visibility into Internet routing errors (and potentially malicious actions) is necessary to support the development of tools like ASPA and BGPsec, and to know when those tools are needed and where they are being deployed effectively. Fastly concurs with the numerous commenters that recommended additional steps to track security measure adoption and identify barriers.[28] Multiple commenters noted the critical role of Internet observatories in providing key data to understand the scope of the problem.[29] More complete data can help understand barriers to adoption and prioritize and coordinate limited expert resources to overcome them. Fastly concurs with the recommendations from several commenters highlighting the need to support Internet observatories[30] and coordinate federal research funding for routing security.[31]

IV. BGPSEC AND ASPA ARE COMPLEMENTARY SOLUTIONS AND EACH HAS CHALLENGES AND OPPORTUNITIES.

[28] Cloudflare Comments at 15.

[29] Comments of Google, PS Docket No. 22-90, at 8-10 (filed Apr. 11, 2022) ("Google Comments").

[30] Comments of Center for Information Technology Policy, PS Docket No. 22-90, at 6-7 (filed Apr. 11, 2022).

[31] Clark Comments at 12-13.

Numerous commentators summarized the potential costs and benefits of BGPsec[32] and ASPA.[33] However, Fastly wishes to clarify the relationship between BGPsec and other tools, and their relative readiness for widespread use. BGPsec prevents path spoofing, while ASPA can prevent route leaks. These are similar but not identical threats that are often conflated. ASPA and BGPsec should not be thought of as mutually exclusive or incompatible; both of these technologies will support routing security in the long term.

BGPsec provides a cryptographic signature that enables a router to verify that the content of the path recorded in a routing message has not been altered by unauthorized parties. Each hop between ASes is verifiable using BGPsec. While BGPsec adoption has been limited by router constraints and cost issues, technological advances in routing hardware and years of investment by providers have advanced and will continue to advance the feasibility of widely adopting BGPsec. There is no "out of the box" solution for BGPsec yet, but they will come.

There are also a number of mitigating factors for BGPsec's "computational overhead." In addition to hardware and software implementation improvements, initial deployments would be most appropriate for high-capacity networks where complete security is worth the costs. While there is still a dearth of software implementation for commercial use of BGPsec, the protocol has been through the IETF standardization process and is fully published as a set of "standards track" RFCs. It has been reviewed by hundreds of subject matter experts over a decade. There are 5 existing BGPsec implementations.[34] We know that it works.

---

[32] Juniper Comments at 7-8.

[33] Comments of CTIA, PS Docket No. 22-90, at 24 (filed Apr. 11, 2022).

[34] *See* BGPsec, *The BGPsec plan*, https://www.bgpsec.net/ (last visited May 9, 2022). The five are: GoBGPsec, NIST-BGP-SRx, ExaBGPsec, BIRD BGPsec, and FRR BGPsec.

But as Google noted in its comments, and Fastly concurs, BGPsec is not a complete solution, because by its nature BGPsec does not prevent route leaks.[35] To address that problem requires a different tool, which is where ASPA comes in. ASPA is an under-development protocol that Fastly has contributed to and that has the potential to improve BGP security in a way complementary to BGPsec, without the need for costly router hardware upgrades.[36] ASPA works by transmitting a list of upstream and downstream AS numbers, so that other ASes can validate the route messages they receive with the public list. ASPA can prevent route leaks, but not path spoofing, because it does not verify the *authenticity* of a path. Unlike BGPsec, ASPA is still under development. It is currently being worked on by the Secure Inter-Domain Routing Operations working group of IETF, which develops guidelines and guidance for deploying secure routing technologies. There are a handful of ASPA implementations under development,[37] but at this point they are still years away from adoption and widespread implementation.

BGPsec and ASPA face distinct challenges: while BGPsec is farther along in terms of being defined as a standard, it requires additional software development and modern hardware for full implementation. Current hardware deployment can support limited (but not ubiquitous) BGPsec deployment. In contrast, ASPA is still being defined—but once the protocol is developed, it can likely be implemented more rapidly, without the need for hardware advances and software development. It is difficult to predict which approach can be more quickly implemented, as they are on separate, independent development paths.

---

[35] Google Comments at 6.

[36] IETF ASPA working draft.

[37] National Institute of Standards and Technology, *BGP Secure Routing Extension (BGP-SRX) Software Suite* (last updated Mar. 10, 2022), https://www.nist.gov/services-resources/software/bgp-secure-routing-extension-bgp-srx-software-suite; CZ.NIC GitLab, *Bird Internet Routing Daemon*, https://gitlab.nic.cz/labs/bird/-/tree/aspa (last visited May 9, 2022).

V. THE FCC SHOULD SUPPORT SECURE ROUTING TECHNOLOGY ADOPTION BUT IT IS PREMATURE TO MANDATE ANY PARTICULAR TECHNOLOGICAL SOLUTION.

A. The Commission has a Significant Role in Raising Awareness and Facilitating Innovation.

The FCC and other U.S. government agencies are key stakeholders in the Internet community. There are several actions the FCC can take to support routing security: the FCC should encourage the federal government to support evangelists for BGPsec, ASPA, and other developing approaches, including through the IETF. The FCC should also support training for network operators on best practices and encourage participation in groups like NANOG. The Commission could support open-source software developers such as OpenBSD in providing BGPsec and ASPA implementations.[38] The FCC could also work within the federal government to promote preferential procurement for network operators that have implemented secure routing.

Routing security improvements take years. A major factor is the hardware investment cycle for providers. As hardware advances, it will be possible to do the more advanced computations necessary for BGPsec. But these advances happen more-or-less predictably as legacy hardware is retired and new hardware is deployed; it is impractical—if not impossible—to attempt to change this cycle or demand that it be done faster. The FCC must recognize the enormity of the challenge for implementing a new protocol across an international provider's networks, and provide the time and attention needed for hardware and software development to move forward and make things like BGPsec possible.

[38] The OpenBSD Foundation, *The OpenBSD Foundation - Funding for OpenBSD and related Projects*, http://www.openbsdfoundation.org/ (last visited May 9, 2022).

B. A Mandatory Approach Would Stifle Innovation and Have Significant Implementation Costs and Challenges.

The Commission should proceed cautiously before taking any regulatory steps to mandate adoption of particular tools or technologies. Neither BGPsec nor ASPA are fully mature and ready for global deployment, and adopting premature regulations could have negative consequences from deploying a technology that is not ready for widespread use. Mandating the implementation of BGPsec now, for example, would involve a years-long project for large enterprise providers and would not be synced with current hardware upgrade deployment or software development schedules.

Further, enshrining a particular solution as a mandate would likely have other negative effects, such as creating "tunnel vision" as the community scrambles to comply, limiting the attention and resources needed to develop other approaches and the next generation of tools. Mandatory implementation of particular tools would also lock providers into existing capabilities and potentially foreclose the development of future advanced solutions, to the detriment of innovation into potentially better routing security.

VI. CONCLUSION

Fastly appreciates the opportunity to add to the record for this important NOI. The Commission has focused on a critical issue for the global Internet, but one that remains the subject of patient, painstaking work over decades by a cadre of dedicated experts. Today's geopolitical realities will require widespread adoption of cryptographically protected routing. To promote increased routing security, the FCC should avoid mandating technological solutions while continuing to foster the global, collaborative, voluntary approach to innovating, and focusing attention and resources on helping train and enhance capabilities for network operators.

Respectfully submitted,

/s/ *David Sando*

David Sando
Vice President & Deputy General Counsel

Job Snijders
Principal Engineer

May 10, 2022