Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

REPLY COMMENTS OF THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

I. INTRODUCTION

The National Telecommunications and Information Administration (NTIA), as the President's principal adviser on telecommunications and information policy,[1] offers this reply comment in the Federal Communications Commission's (Commission's) Notice of Inquiry in the Matter of Secure Internet Routing (NOI).[2] The security of communications is a vital concern, and NTIA appreciates the undertaking by the Commission to solicit public comments on Border Gateway Protocol (BGP) security vulnerabilities. Malicious BGP activity as well as inadvertent BGP anomalies are tremendously detrimental. To address these security vulnerabilities, NTIA has several suggestions for the Commission.

NTIA recommends that the Commission continue to engage multistakeholder fora such as the Communications Security, Reliability, and Interoperability Council (CSRIC) and supports continued U.S. government (USG) interagency coordination on secure Internet routing and collaboration with the private sector. NTIA supports, in particular, several recommendations

[1] 47 U.S.C. § 902(b)(2)(D).

[2] *In the Matter of Secure Internet Routing*, PS Docket No. 22-90, Notice of Inquiry, FCC 22-18 (rel. Feb. 28, 2022) ("NOI").

submitted in the first round of comments, including the proposals urging sustained research on BGP security and resilience, as well as guidance and support for network operators, Internet Exchange Providers, Content Delivery Networks and cloud providers, and equipment vendors, to bolster BGP security practices. NTIA notes the many comments submitted that recommend non-regulatory approaches for Internet technical issues. Finally, NTIA agrees with those comments urging the USG to ensure that its own networks and procurement requirements reflect BGP security best practices.

II. THE COMMISSION SHOULD CONTINUE WORKING WITH CSRIC TO STUDY THE BEST METHODS OF COOPERATION AND COORDINATION

The Commission's Federal Advisory Committee–the Communications Security, Reliability, and Interoperability Council[3]—is a multistakeholder forum that has advised the Commission on network reliability and security. By taking a voluntary approach to studying BGP security through CSRIC, the Commission has demonstrated that it can successfully coordinate and cooperate with stakeholders to respond to network security concerns. The Commission should continue to work with CSRIC to improve cybersecurity and BGP security.[4]

[3] Communications Security, Reliability and Interoperability Council, Federal Communications Commission, www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited May 9, 2022).

[4] Cisco Comments at 13 ("Tasking the Communications Security, Reliability, and Interoperability Council (CSRIC) to update its best practice recommendations. Even in just the few years since the latest CSRIC report on this topic, there have been material technological and operational developments relevant to routing security. ASPA has entered the process of standardization, the MANRS Observatory has been launched, numerous open-source tools have been developed to ease the adoption of the RPKI and BMP, and the multiplicity of private peering models for both cloud and enterprise connectivity have increased. A detailed CSRIC analysis that explores the trade- offs and recommendations for different kinds of interconnection scenarios could prove valuable as organizations of different kinds evaluate how to improve their routing security postures.").

CSRIC is comprised of representatives from network services, vendors, academia, researchers, consumer groups, government, Internet governance organizations, and others. In the past, the Commission has referred challenging questions regarding network reliability and security practices to CSRIC. In response, CSRIC has developed network reliability and security best practices, provided expert guidance to the Commission and coordinated responses to network vulnerabilities. Voluntary compliance with these best practices has effectively improved network security and reliability.[5]

Additionally, CSRIC reviews a network's implementation of best practices, reviews what was effective, considers where failure to implement best practices led to problems, revises the best practices, and makes recommendations to the Commission. The Commission has effectively used CSRIC to study and coordinate responses to network vulnerabilities, and CSRIC has provided the Commission with expert guidance.

CSRIC has a long history of applying its expertise to BGP and related matters and can continue to do so effectively. In 2013, the Commission convened CSRIC III to report on, among other things, "the reliability and security of communications systems and infrastructure."[6] Final reports from CSRIC working groups included expert information, recommendations, and best

[5] *See, e.g.*, *Analysis of the Effectiveness of Best Practices Aimed at E911 and Public Safety*, Final Report, NRIC VII (Dec. 2005), transition.fcc.gov/nric/nric-7/fg1c-report.pdf; *Wireless Network Reliability*, NRIC VII Focus Group 3A Final Report (Sept. 2005), transition.fcc.gov/nric/nric-7/fg3a-report.pdf (conducting survey and concluding that best practices are effective).

[6] Charter of the Communications Security, Reliability and Interoperability Council, Federal Communications Commission (2013), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC%20Charter%20Renewal%202011%20FINAL.pdf (CSRIC III also reported on issues related to 911, Enhanced 911 (E911), and Next Generation 911 (NG911), and emergency alerts).

practices on BGP security.[7] Within the greater context of cybersecurity, CSRIC recommended coordination and cooperation with various fora and noted that, because BGP security is an evolving field, the best practices recommended had limitations.

After CSRIC III, stakeholders came together to create Mutually Agreed Norms for Routing Security (MANRS), referencing the work of the National Institute for Standards and Technology (NIST), CSRIC, and others to promote BGP security best practices.[8] NTIA supports MANRS as a voluntary initiative to elevate globally the status of BGP security.

In 2019, the Charter of CSRIC VI asked the group "to report on the Best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols."[9] CSRIC reviewed its recommendations, IETF developments, MANRS, NIST guidance, and National Security Agency (NSA) guidance. CSRIC VI noted that cybersecurity is an evolving environment. It recommended further research and promotion of best practices, implementation of NSA best practices, implementation of Route Origin Validation, participation in MANRS, participation in and review of NIST guidance, registration of network address resources in Internet Routing Registries, and certifying number resources with Regional Internet Registries (RIRs). Significantly, CSRIC VI did not indicate a need for regulatory intervention.

---

[7] *Network Security Best Practices*, CSRIC III Working Group 4 Final Report (Mar. 6, 2013), https://www.fcc.gov/pshs/advisory/csric3/4%20WG%20Presentation%2003-06-13.ppt; *Secure BGP Deployment*, CSRIC III Working Group 6 Final Report (2013), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_%202013.pdf.

[8] MANRS for Network Operators, Version 2.5.2 (May 17, 2021), https://www.manrs.org/isps/ (last visited May 8, 2022).

[9] *Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP based Protocols*, CSRIC VI Final Report (Mar. 2019), https://www.fcc.gov/files/csric6wg3finalreport030819pdf.

Engagement through CSRIC has proven effective in developing and coordinating a cybersecurity response. This history supports commenters' arguments that the industry can best respond to BGP security by continuing to implement BGP solutions and best practices and continuing to participate in multistakeholder efforts such as MANRS.[10] As such, the Commission should consider continuing to leverage CSRIC to address cybersecurity concerns.

III. THE COMMISSION SHOULD COORDINATE WITH OTHER FEDERAL AGENCIES ALREADY WORKING ON BGP SECURITY POLICY

NTIA concurs with commenters who cited the newly relaunched Cybersecurity Forum for Independent and Executive Branch Regulators, for which Commission Chairwoman Jessica Rosenworcel serves as the Chair, as a particularly useful forum for coordinating BGP security with other federal entities.[11]

[10] *See, e.g.*, Google Comments at 2 ("BGP stakeholders should adopt relevant MANRS recommendations"); Geoff Huston Comments at 5 ("It is unrealistic to require every network operator to be in a position to make a thoroughly informed response to such questions, and programs that outline a set of common practices for network operators to adopt and accompany such practice descriptions with rationales and pointers to additional information undertake a valuable role. In this respect MANRS offers a well-structed and carefully thought through approach to best current practices in routing security and is clearly the best program in the industry today in this area."); IAB Comments at 2 ("We believe in a continuous, modular, flexible evolution of the Internet and its protocols based on operational experience and requirements, where each service provider can determine their security needs based on their diverse requirements and in partnership with other providers. The success of future standardization efforts intended to increase routing security, we believe, will be highly dependent on educating BGP users about BGP operational issues and how well real-world deployment experience can be fed back into the multistakeholder standards development process, as opposed to a mandated top-down approach, which would fail to meet the diverse needs of the global community."); Cloudflare Comments at 1 & 14 ("we recommend that the Commission encourage continued adoption of existing best practices without using regulatory authority to achieve compliance with any of the routing security methods." "We do not believe regulatory mandates on BGP security are appropriate.").

[11] *See* Press Release, Federal Communications Commission, Chairwoman Rosenworcel to Lead Federal Interagency Cybersecurity Forum (Feb. 3, 2022), https://www.fcc.gov/document/chairwoman-rosenworcel-lead-federal-interagency-cybersecurity-forum; Google Comments at 7 ("As recently highlighted by Chairwoman Rosenworcel's reconvening and leading the Cybersecurity Forum for Independent and Executive Branch Regulators, the Commission can support "a whole-of-government approach to cybersecurity.").

In addition, the Commission should continue to work with other USG entities that have relevant expertise and responsibilities concerning BGP security, including NTIA, NIST, the Department of Homeland Security through the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA),[12] the Department of Defense (DOD), the National Science Foundation (NSF), other federal entities, the federal IT community through the Office of the Federal Chief Information Officer, and the Federal Chief Information Officers Council.[13]

The Commission should coordinate with NIST if it has questions or seeks guidance concerning resilient interdomain traffic exchange.[14] Pursuant to the Federal Information Security Modernization Act (FISMA),[15] NIST is responsible for developing information security standards and guidelines, including minimum requirements, for federal information systems. To do so, NIST engages various communities, including the interagency, industry, and academia, and provides technical guidance and recommendations for technologies that facilitate resilient interdomain traffic exchange.

---

[12] *See*, *e.g.*, National Security Agency, *Cybersecurity Report: A Guide to Border Gateway Protocol (BGP) Best Practices.* U/OO/202911-18 PP-18-0645 (Sep. 10, 2018), https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/ctr-guide-to-border-gateway-protocol-best-practices.pdf.

[13] Clark, Claffy Comments at 13 ("There are multiple agencies in the U.S. government that have some current or potential role in improving Internet security. We believe that the FCC can be most effective as part of cross agency coalitions that work in a coordinated fashion.").

[14] As noted, the FCC's CSRIC consulted with NIST when it produced its guidance on BGP security. See *Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP based Protocols*, CSRIC VI Final Report (Mar. 2019), https://www.fcc.gov/files/csric6wg3finalreport030819pdf. In other proceedings that have referenced BGP security concerns, such as the recent Chinese telecommunications proceedings, the FCC has cited NIST as its expert authority for its arguments concerning BGP vulnerabilities. *See* 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 Telecom (Americas) Corporation, Order on Revocation and Termination, GN Docket No. 20-109, FCC 21-114 (Nov. 2, 2021); China Unicom (Americas) Limited, Order on Revocation, GN Docket No. 20-110, FCC 22-9 (Feb. 2, 2022).

[15] Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551, *et seq*.

NIST has released key documentation on, and tools for, secure routing. Specifically, *NIST SP 800-189, Resilient Interdomain Traffic Exchange—BGP Security and DDoS Mitigation*,[16] provides technical guidance and recommendations for deploying technologies that improve the security of interdomain traffic exchange. It focuses on securing the interdomain routing control (i.e., BGP) traffic as well as mitigating DDoS attacks. This document applies to enterprise networks and the network services of hosting providers (e.g., cloud-based applications and service hosting) and Internet service providers (ISPs) that support them. NIST also recently published *NIST Technical Note 2060, BGP Secure Routing Extension (BGP-SRx): Reference Implementation and Test Tools for Emerging BGP Security Standards.*[17] NIST has also made available *BGP the Secure Routing Extension (BGP-SRx) Software Suite*, an open source reference implementation and research platform for investigating emerging BGP security and robustness extensions and supporting protocols such as RPKI Origin Validation, BGPsec Path Validation and Route Leak Detection and Mitigation schemes.[18]

Through collaborative efforts with industry at the National Cybersecurity Center of Excellence, NIST has also been evaluating emerging technologies and best practices. For example, the Secure Inter-Domain Routing project, used commercially available technologies to demonstrate the practicality of BGP Route Origin Validation, leveraging the Resource Public

[16] Kotikalapudi Sriram & Doug Montgomery, *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation,* NIST S.P. 800-189 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189.pdf ("NIST SP 800-189").

[17] Borchert, Oliver, et al., *BGP Secure Routing Extension (BGP-SRx): Reference Implementation and Test Tools for Emerging BGP Security Standards,* NIST Technical Note 2060 (Sept. 2021), https://csrc.nist.gov/publications/detail/white-paper/2021/09/15/bgp-secure-routing-extension-bgp-srx/final.

[18] BGP Secure Routing Extension (BGP-SRx) Software Suite, NIST, https://www.nist.gov/services-resources/software/bgp-secure-routing-extension-bgp-srx-software-suite (last visited May 5, 2022).

Key Infrastructure (RPKI) to address and resolve the erroneous exchange of network routes.[19] Several organizations with relevant capabilities have agreed to collaborate with NIST through a Cooperative Research and Development Agreement (CRADA) to build this example solution.

The Commission also should coordinate with NTIA. Among other responsibilities, NTIA is by statute the President's principal adviser on telecommunications and information policy.[20] NTIA also is the Executive Branch expert on the USG's multistakeholder approach to Internet governance. NTIA represents the United States on the Governmental Advisory Committee of the Internet Corporation for Assigned Names and Numbers (ICANN). If the Commission has questions concerning ICANN, RIRs, or other issues related to Internet governance, NTIA would welcome close coordination.

The NSF is another key governmental stakeholder. The NSF funds research into BGP security, which should be a critical input to any Commission activities in this area.[21]

The Commission also should continue to work with NTIA and the State Department to engage international policymakers, particularly on the question of BGP security to ensure that Commission policy is consistent with USG policy. For example, the USG has long promoted

---

[19] Secure Inter-Domain Routing, Nat'l Cybersecurity Ctr. of Excellence, Nat'l Inst. of Standards & Tech., https://www.nccoe.nist.gov/projects/building-blocks/secure-inter-domain-routing (last visited May 8, 2022).

[20] *See* 47 U.S.C. § 902(b)(2)(D) (conferring on NTIA "[t]he authority to serve as the President's principal adviser on telecommunications policies pertaining to the Nation's economic and technological advancement and to the regulation of the telecommunications industry.").

[21] *See, e.g.,* Award Abstract #1117052 TC: Small: Collaborative Research: Towards a Formal Framework for Analyzing and Implementing Secure Routing Protocols CNS Division of Computer and Network Systems 2011 Investigator(s): Boon Thau Loo. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1117052; Award Abstract #0721736 Collaborative Research: NETS-NBD: RIDR: Towards Robust Inter-Domain Routing: Measurements, Models, and Deployable Tools CNS Division of Computer and Network Systems Investigator(s): Christos Faloutsos 2007, https://www.nsf.gov/awardsearch/showAward?AWD_ID=0721736. *See also* Experimental Deployment of the ARTEMIS BGP Hijacking Detection Prototype in Research and Educational Networks, CAIDA (2018), https://www.caida.org/funding/eager-artemis/ (last visited May 8, 2022) (funded by the National Science Foundation).

and, in international fora defended, the open development of Internet technical standards through multistakeholder deliberation, debate, and, ultimately, a consensus-based decision-making process.[22] The Internet's success over time is testament to the wisdom of the multistakeholder approach, which the Biden Administration reaffirmed last month in the *Declaration for the Future of the Internet*.[23] In contrast to this vision, authoritarian governments have sought and continue to seek to establish intergovernmental control over Internet standards and governance in multilateral fora.[24] Regulation by the Commission over Internet routing could set a damaging precedent in support of international Internet regulation, in contrast to standing USG policy.

The USG has multiple stakeholders throughout numerous agencies and offices working on BGP security. It is imperative that such work is consistent and coordinated. The Commission should be sure to coordinate any BGP-related activities it pursues with other federal entities.

---

[22] *See Connecting America: The National Broadband Plan*, FCC Report, Rec. 16.9, p. 322 (2010) ("The FCC should increase its participation in domestic and international fora addressing international cybersecurity activities and issues.") ("FCC Broadband Plan").

[23] Fact Sheet, White House, United States and 60 Global Partners Launch Declaration for the Future of the Internet (Apr. 28, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/28/fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet/ ("Multistakeholder Internet Governance [includes obligations to:] Protect and strengthen the multistakeholder system of Internet governance, including the development, deployment, and management of its main technical protocols and other related standards and protocols [and to] Refrain from undermining the technical infrastructure essential to the general availability and integrity of the Internet.").

[24] *See, e.g.*, Contribution by the Russian Federation, Council Working Group on International Internet-related Public Policy Issues, Doc. CWG 15/6, at 1 (Jan. 14, 2021) ("Given the fact that ITU is a specialized technical agency of the United Nations, it seems appropriate to discuss the role of ITU and Member States in ensuring trust and security in the Internet at the international level and to adopt framework agreements regarding the technical aspects of regulating the security of the critical infrastructure of the global Internet space."), https://www.itu.int/dms_pub/itu-s/md/21/rclintpol15/c/S21-RCLINTPOL15-C-0006!!MSW-E.docx; Report on the Seventeenth Meeting of the Council Working Group on International Internet-Related Public Policy Issues (CWG-Internet), at 2-3 Doc CWG-Internet 17/6 (Jan. 24, 2022) ("The Russian Federation highlights two main dangerous issues for operation of the critical Internet resources: firstly, the dependence of organization/operators of critical Internet infrastructure providing over national functions on the decisions of one national administration has turned from a potential threat into a real fact; secondly, the growth of autonomous, unsynchronized national initiatives on Internet regulation, while mandatory for the cross-border application.").

IV. INTERNET TECHNICAL ISSUES ARE BEST ADDRESSED THROUGH COORDINATION WITH A VARIETY OF STAKEHOLDERS

Stakeholders in comments to this NOI identify issues with BGP security and its implementation. Because the challenges to adoption of BGP security practices are outlined in the comments and in literature, we do not repeat that extensive material here. However, we note some concerns in order to assess the problem at which the NOI is aimed, and to observe that the best method of addressing that problem is through multistakeholder fora.

Although some solutions are effective even if implemented by only a portion of the network community,[25] others require substantial or uniform implementation by the community before a benefit can be realized. This is a collective action problem,[26] in which there is a disincentive for any one network to make an investment and be the first mover implementing a solution. This is also known as a commons problem, where the investment of one firm may benefit the whole community but the benefit gained by that individual firm is limited, unless the other members of the community act as well.[27] Commenters also note other problems with incentives to deploy security.[28]

---

[25] NIST S.P. 800-189, Sec. 1.3 ("The creation of ROAs can be accomplished independently by each address resource holder, and ROV can be deployed by each AS independently. Thus, there is clearly a benefit for early adopters, and deployment grows in a distributed manner.").

[26] Verizon Comments at 2 ("The global, interconnected, distributed nature of the Internet means that there are significant limits to the security or reliability benefits that any single stakeholder or group of stakeholders can unilaterally bring about.").

[27] Clark Claffy Comments at 4 ("Misaligned incentives for actors. ISPs will almost certainly bear the major cost and complexity of deploying a change to BGP, but they are not the beneficiaries of the changes. It is primarily the end points that benefit, not the ISPs, that benefit from reduced hijacks.").

[28] Juniper Comments at 5 ("The primary outstanding concern about further deployment lies in a disconnect between ISP costs and benefits. Normally, ISPs are not major producers or consumers of Internet content; they only provide conveyance for packets between users and content providers. As a result, when there is a BGP hijacking attack, content consumers and providers are impacted, but the ISP typically sees little to no economic impact. Conversely, when deploying any BGP security mechanism, ISP costs are deeply impacted while content consumers are not

In addition to lagging adoption, there is a need for improvement of measurement and monitoring tools. Current measurement and monitoring tools may be incomplete and therefore the assessment of the problem and the effectiveness of solutions is largely anecdotal.[29]

Commenters observe that security solutions, and specifically BGP security solutions, mitigate the problem rather than solve it.[30] BGP interconnection relationships are complex.[31] BGP security solutions are also complex and incomplete, and as a result, may even introduce new vulnerabilities.[32] Some BGP security solutions are computationally resource demanding and become increasingly more demanding as implementation scales.[33] Security requires costly investments, placing significant demands on limited budgets.[34]

---

impacted, and content providers are somewhat impacted. This creates a motivational deficit for the ISP: deploying BGP security mechanisms has clear costs that are not offset by direct benefits. The benefits accrue only to the content consumers and providers, the majority of whom are not the ISP's direct customers."); Clark, Claffy Comments Sec. 3 ("ISPs will almost certainly bear the cost and complexity of deploying a change to BGP, but they are not the beneficiaries of the changes. It is the primarily the end points that benefit, not the ISPs, from reduced hijacks.").

[29] Geoff Huston Comments at 2 ("We still rely on anecdotes of individual incidents to illustrate the relative insecurity of the inter-domain routing environment and have been frustrated in efforts to place such incidents into the broader context of the number of such impacts and their scope and impact.").

[30] Juniper Comments at 9 ("Network operators can partially mitigate the threat of BGP attack by deploying all the Mutually Agreed Norms for Routing Security (MANRS) recommendations, including TCPAO and RPKI. They can also detect route hijacks using tools like ARTEMIS.").

[31] Cisco Comments at 6 ("The diversity of neighboring relationships that BGP supports is a major challenge to securing BGP.").

[32] Geoff Huston Comments at 1 ("none of these are necessarily complete and robust. Not only have these proposals not addressed the complete set of potential vulnerabilities that are known to exist in the operation of BGP, but to various extents these proposals appear to introduce new vulnerabilities into the operational environment. It would be imprudent to consider the current state of BGP security mechanisms, as encompassed by the sole use of RPKI, Route Origination Validation and BGPSEC as complete and fully ready for broad scale deployment, and the cautious stance taken by many operators of Internet infrastructure with respect to deployment of these tools is reflective of a level of due consideration relating to adoption of new technologies where the risks and vulnerabilities of the technology are still not fully appreciated."). *Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation*, NIST Spec. Pub. 1800-14A (June 2019), https://www.nccoe.nist.gov/sites/default/files/legacy-files/sidr-nist-sp1800-14a-final.pdf.

[33] Juniper Comments at 6; Geoff Huston Comments at 4.

[34] Juniper Comments at 8.

The purpose of noting commenters' identification of challenges is not to endorse their views or suggest that BGP security is problematic, but to identify the type of challenges confronting this work. It is also to observe that the proven best way to respond to and address these problems is through coordination with a variety of stakeholders and fora that have the expertise and perspectives necessary to identify, create, recommend, or implement solutions. In order to explore and attempt to resolve these potential complex problems, broad input and consideration from interested parties is required. The Commission has embraced and supported a multistakeholder approach in the past and should continue to do so.

NTIA notes commenters and relevant literature suggest that regulations to address BGP security would be ineffective and that regulatory mandates could inadvertently impede security efforts. Questions of BGP security regulation should be considered in the larger context of cybersecurity regulation. As commenters note, a holistic approach needs to be developed.[35] Security concerns are complex, with interrelated issues and solutions.[36] Responses to BGP security are going to have commonalities with DNS security as well as supply chain security,

[35] Verizon Comments at 5 ("Internet routing security should be considered within the context of the broader set of cybersecurity threats and mitigation tools."); Clark, Claffy Comment at 13 ("BGP is only part of the story about Internet security. An effective approach will look at the abuses of the various systems of the Internet—the abuse of addresses, abuse of BGP, abuse of the DNS, abuse of the Certificate Authority system—in a holistic way."); Comments of ARIN at 2 ("the Commission may wish to consider the Internet security requirements included in the variety of Internet services that the FCC specifies or purchases to the extent that the security of their Internet routing is a concern."); Juniper Comments at 7 ("Overall security requires global cooperation, and regulating only one small portion of the problem, while helpful, is not ultimately a solution.").

[36] Juniper Comments at 5. ("Internet security is a broad and complex topic. The aforementioned mechanisms are specific to the Internet's routing subsystem. Many other threats to critical subsystems are not addressed by these mechanisms, such as attacks on the Domain Name System (DNS), ISP intrusion, and attacks on the Internet's data plane or forwarding plane. Data plane attacks are threats that compromise the privacy or integrity of packets as they flow through the Internet. For example, an attacker could place a tap on an Internet link and make a copy of each packet, compromising end-user privacy. This pervasive monitoring is not addressed by any BGP security mechanism. Attackers could also create 'detours' within the forwarding plane, where traffic is re-routed and then possibly copied, modified, or removed from the data stream. The remaining traffic could be re-injected into the data path, making threat detection very difficult. Subtle attacks, such as decreasing the performance of a specific data flow are also possible. None of the routing plane security mechanisms help counter these data plane threats.").

denial of service attacks, interception of traffic, theft of data and information, man-in-the middle attacks, botnets, and the full field of cybersecurity concerns. NIST guidance states that in order to be effective, cybersecurity must be approached systematically and holistically.[37] The Commission's National Broadband Plan recommended that the Commission first establish a cybersecurity roadmap that provides "a clear strategy for securing the vital communications networks."[38] There is no one silver bullet solution to cybersecurity, and addressing issues individually through regulation risks limiting the effectiveness of the response.

Both stakeholders and cybersecurity literature identify serious problems associated with regulatory intervention in cybersecurity and specifically with BGP security. We will not repeat all of the concerns raised by commenters here, but we will review some of them to scope out the problems that could result from regulatory mandates of specific BGP security tools and protocols. For example, comments note that a regulatory mandate risks locking in today's solution while failing to address tomorrow's threats.[39] Meanwhile, cybersecurity requires a nimble flexible posture on the part of network operators. By mandating specific solutions, the ability to be flexible in response to threats may be reduced.

Furthermore, other federal agencies, CSRIC;[40] MANRS, ARIN, the IETF, the ICANN

[37] *See also* Verizon Comments at 2 ("Service providers must thus deploy a comprehensive, layered approach to security that assumes the persistence of Border Gateway Protocol ("BGP") routing and other Internet route hijacking risks, and must deploy tools to efficiently detect, respond to, and recover from hijacking incidents.").

[38] FCC Broadband Plan, Rec. 16.5, p. 321.

[39] Cisco Comments at 1 ("Regulatory action, by contrast, would be an untested approach that risks locking the industry into ineffective technologies and imposing a one-size-fits-all scheme while having limited impact due to the global nature of the system.").

[40] *Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP based Protocols*, CSRIC VI Final Report (Mar. 2019), https://www.fcc.gov/files/csric6wg3finalreport030819pdf ("MANRS is an important organization addressing routing security globally that is endorsed by CSRIC VI WG 3.").

community,[41] the Internet Society,[42] RIRs; and foreign governments have embraced promoting BGP security best practices and have not sought a regulatory solution.[43] USG policy in international fora advances multistakeholder solutions rather than regulatory intervention, and NTIA recommends the Commission pursue this approach at the domestic level as well. The record and literature do not present evidence that regulatory intervention would be beneficial for BGP or cybersecurity purposes.

V. THE COMMISSION SHOULD FOCUS ON NON-REGULATORY RESPONSES AND SUPPORT RESEARCH & DEVELOPMENT EFFORTS

Commenters and literature have identified non-regulatory USG responses that could be directed toward improving BGP security. The USG has a long history of supporting research and development focused on improving the evolution, security and robustness of core Internet infrastructure and protocols.[44] Basic research on future Internet architectures is led by the NSF. [45] NIST, through its "Trustworthy Networks Program," has led USG applied research efforts to design, standardize, and foster adoption of technologies to improve the security and resilience of

[41] *DNS Security Facilitation Technical Study Group*, Final Report, ICANN p. 34 (2021), https://community.icann.org/display/DSFI/DSFI+TSG+Final+Report?preview=/176623416/176623417/DSFI-TSG-Final-Report.pdf (Rec. E4, recommending continued participation in MANRS).

[42] *See* About MANRS, MANRS, https://www.manrs.org/about/ (last visited May 8, 2022) ("Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society.").

[43] *See, e.g., 7 Steps to Shore Up BGP*, ENISA (May 2019), https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp; *Technical Report: Responsible Use of the BGP for ISP Networking*, UK National Cyber Security Centre (2021), https://www.ncsc.gov.uk/files/border-gateway-protocol-technical-paper.pdf.

[44] Andrew Gallo Comments at 2 ("I encourage the Commission, either unilaterally or in partnership with other federal entities, to fund (or continue to fund) important efforts such as CAIDA's Spoofer6, BGPStream7, and ARTEMIS, along with the University of Oregon's RouteViews9 project"); Clark, Claffy Comments at 10 ("The CAIDA BGPstream service takes in data from RouteViews and RIPE and makes it available in a more convenient and easy-to-use form. At the moment, CAIDA has no funding to sustain BGPstream, and continues to support it in the hopes that more stable funding will emerge."); Intrusion *ex parte* at 2.

[45] NSF Future Internet Architecture Project, NSF, http://www.nets-fia.net/ (last visited May 8, 2022).

the current Internet's foundational protocols. [46] NIST has worked closely with Internet industry groups (e.g., IETF, North American Network Operators Group (NANOG)) to design, standardize and foster adoption of a range technologies to improve the security and resilience of BGP. NIST technical contributions include IETF standards development, reference implementations and test systems for vendors, deployment guidance and technology demonstrations and global measurement and monitoring systems for network operators designed to foster trust in new BGP security mechanisms.[47] Both the Department of Homeland Security and the Department of Defense support security research and implementation.

The first generation of standardized BGP security technologies (i.e., the resource public key infrastructure (RPKI) and route origin validation (ROV)) are commercially viable and are being deployed across the global Internet. Adoption in North America, and by the USG is lagging that of Europe,[48] suggesting that further efforts to facilitate adoption should be considered.

Technologies to address other issues in BGP security and resilience (e.g., full BGP path validation (BGPsec), route-leak mitigation, DDoS mitigation) require continued USG support and involvement to complete their standardization, develop additional adoption guidance, and advance their operational deployment.

[46] NIST Trustworthy Networks Program, NIST, https://www.nist.gov/programs-projects/trustworthy-networks-program (last visited May 8, 2022).

[47] NIST Robust Inter-Domain Routing Project, NIST, https://www.nist.gov/programs-projects/robust-inter-domain-routing (last visited May 8, 2022).

[48] NIST RPKI Monitor, NIST, https://rpki-monitor.antd.nist.gov/ (last visited May 8, 2022).

Commenters suggest that the Commission consider how it can best support research and implementation through non-regulatory means.[49] We agree and believe that potential areas for exploration include:

- Should BGP security be made a part of "Measuring Broadband America" or other data gathering projects?[50]
- Should the Network Outage Reporting System include impacts created by BGP anomalies?
- Should funding for BGP security be identified as part of the Commission's universal service programs?[51]
- Can the Commission help defray the costs of security for networks serving unserved or underserved markets?
- Can the Commission reduce the costs of security for smaller networks through the promotion of CSRIC, NIST, and other expert best practices and guidance?
- Can the Commission engage in educational outreach to promote implementation of solutions?[52]

[49] *See* NIST SP 800-189, Sec. 8.5 ("Additional research is needed to determine how ROV-capable routers should best use the ROV evaluation state in the route selection policy... researchers affiliated with NIST and the IETF Working Group are investigating this question.).

[50] Cloudflare Comments at 14.

[51] Cisco Comments at 14; Cloudflare Comments at 15.

[52] Juniper Comments at 5 ("Further educational and motivational efforts for both RPKI and TCP-AO would continue to be helpful to promote and accelerate deployment"); IAB Comments at 2 ("The Federal Communications Commission can support the efforts of the Internet community to deploy mechanisms to secure global routing by supporting research and other work that help these communities to understand issues, develop solutions where needed, and deploy security technology more widely.); Internet2 Comments at 7 ("The Commission, and related arms of the federal government, can play a role in helping to educate the R&E community that good routing security is critical to its network-centric infrastructure."); Cloudflare Comments at 14 ("promote best practices around BGP security"). *See also* NIST SP 800-189, Sec. 8.2 (discussing follow on activities including demonstration activities of developing solutions).

The Commission should state support for future research and development efforts led by NIST, NSF, and others to advance the state of BGP security technology, including relevant standards and guidance. While the USG was the driving force behind the most recent development of commercially viable, standardized BGP security extensions–the first in 30 years–further work is needed to improve the robustness and utility of these features to advance the state of their deployment.

VI. THE U.S. GOVERNMENT CAN LEAD BY EXAMPLE

The Commission should work with NIST and other federal entities responsible for USG BGP security policy and resource management, including those empowered to coordinate the removal of both operational and policy barriers to BGP security technology adoption. The majority of USG networks have not deployed emerging BGP security technologies, leaving our critical network infrastructures vulnerable to an increasing range of attacks.[53] However, the USG can lead by example starting today.[54]

We recommend undertaking a coordinated effort to expedite adoption of emerging BGP security technologies, starting with USG networks. Broad USG adoption would raise the security of government-to-government, inter-domain communications, and it would serve as an important market catalyst to foster broader development of commercial offerings for BGP security technologies.[55] Beyond the enhanced security benefits for USG IT assets, the nature of emerging

[53] *See* Aftab Siddiqui, *What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets*, Internet Society (Apr. 27, 2018), https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/ (BGP attacks are often the first step in attacks on other infrastructure such as DNS, PKI, email, etc.).

[54] Cisco Comments at 14 ("Improving the adoption of BGP security technologies on existing federal government networks. The publication of ROAs and the adoption of origin validation is an ongoing process across the federal government's existing ASN footprint. The U.S. government has an opportunity to lead by example here").

[55] Cloudflare Comments at 14; Google Comments at 2; Clark, Claffy Comments at 8 ("We can imagine using government procurement regulations to establish MANRS-like requirements for networks operated by or for government agencies, such as occurred for DNSSEC.").

routing security approaches implies a spillover effect such that the neighboring systems of a protected system gain some benefit as well. Given that the USG has a significant number of autonomous system networks and is assigned a significant portion of the Internet address space that is announced through BGP, wide scale adoption of emerging BGP security technologies by USG network operators would significantly advance the national, regional, and global state of deployment, offering an opportunity to raise the security posture of not just implementers, but those around them, which, in and of itself, is a public service that the USG is uniquely positioned to pursue today.

VII. CONCLUSION

The security of communications is a vital concern. Progress on BGP security can be meaningfully and sustainably achieved through coordination with a variety of stakeholders such as the CSRIC. NTIA recommends that the Commission coordinate and cooperate with other U.S. government entities that have expertise and responsibilities concerning BGP security, information resource management, and Internet governance. Finally, we believe that the Commission should consider the many non-regulatory responses to the identified concerns.

Respectfully submitted,

Milton Brown

Milton Brown
Chief Counsel (Acting)

National Telecommunications and
Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230
202-482-1816

May 10, 2022