Dated: June 11, 2024.

Lauren K. Roth,

Associate Commissioner for Policy.

[FR Doc. 2024–13236 Filed 6–14–24; 8:45 am]

BILLING CODE 4164–01–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 1

[PS Docket Nos. 24–146, 22–90; RIN 3060–AL83; FCC 24–62; FR ID 225236]

Reporting on Border Gateway Protocol Risk Mitigation Progress; Secure Internet Routing

AGENCY: Federal Communications Commission

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) seeks to increase the security of the information routed across the internet by proposing certain reporting obligations on providers of broadband internet access service (BIAS providers) and their use of the Border Gateway Protocol (BGP). Internet traffic can be disrupted, intercepted, and blackholed—when a service provider drops traffic addressed to a targeted IP address or range of addresses by redirecting it to a null route—due to either accidental or deliberate adversarial manipulation of security vulnerabilities inherent to BGP. Together, the intended effect of the plans, filings, and measures the Commission proposes would be to mitigate such threats. BIAS providers would be required to develop BGP Routing Security Risk Management Plans that describe their plans for and progress in implementing security measures that utilize the Resource Public Key Infrastructure (RPKI). Nine of the largest service providers would be required to file specific additional data on a quarterly basis. The FCC also seeks comment on issues related to implementing RPKI-based security measures.

DATES: Comments are due on or before July 17, 2024 and reply comments are due on or before August 1, 2024. Written comments on the Paperwork Reduction Act proposed information collection requirements must be submitted by the public and other interested parties on or before August 16, 2024.

ADDRESSES: You may submit comments, identified by PS Docket Nos. 24–146 and 22–90, by any of the following methods:

- *Federal Communications Commission's website: https://www.apps.fcc.gov/ecfs/.* Follow the instructions for submitting comments.
- *Mail:* Parties who choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number. Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission. Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701. U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE, Washington, DC 20554.

Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID–19. *See FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy,* Public Notice, DA 20–304 (March 19, 2020). *https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.*

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

FOR FURTHER INFORMATION CONTACT: George Donato, Associate Division Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418–0729, or by email to *george.donato@fcc.gov;* or James Zigouris, Attorney-Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418–0697, or by email to *james.zigouris@fcc.gov;* or Bradley Rosen, Attorney-Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418–0226, or by email to *bradley.rosen@fcc.gov.* For additional information concerning the Paperwork Reduction Act information collection requirements contained in this document, send an email to *PRA@fcc.gov* or contact Nicole Ongele, Office of Managing Director, Performance Evaluation and Records Management, 202–418–2991, or by email to *PRA@fcc.gov.*

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's *Notice of Proposed Rulemaking (NPRM),* PS Docket Nos. 24–146 and 22–90; FCC 24–62, adopted June 6, 2024, and released June 7, 2024. The full text of this document is available by downloading the text from the Commission's website at: *https://www.fcc.gov/document/fcc-proposes-internet-routing-security-reporting-requirements-0.* When the FCC Headquarters reopens to the public, the full text of this document will also be available for public inspection and copying during regular business hours in the FCC Reference Center, 45 L Street NE, Washington, DC 20554. To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an email to *FCC504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530 (voice), 202–418–0432 (TTY).

Ex Parte Rules—Permit-But-Disclose: This proceeding shall be treated as a ''permit-but-disclose'' proceeding in accordance with the Commission's *ex parte* rules, with a limited exception described in the following paragraph. 47 CFR 1.1200, 1.1206. 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 § 1.1206(b). In proceedings governed by § 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.,* .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

In order to facilitate the free exchange of exploratory ideas among the staff of the federal agencies working toward the critical goal of promoting secure internet routing, we find the public interest requires a limited modification of the *ex parte* status in this proceeding. *See* 47 CFR 1.1200(a). Communications between the Commission staff and staff of the Federal Government entities with a formal role in these internet security matters, *i.e.,* Office of the National Cyber Director (ONCD), Cybersecurity and Infrastructure Security Agency (CISA), Department of Justice (DOJ), Office of the Director of National Intelligence, National Institute of Standards and Technology (NIST), and National Telecommunications and Information Administration (NTIA) shall be exempt from the rules requiring disclosure in permit-but-disclose proceedings and exempt from the prohibitions during the Sunshine Agenda period. *See generally* 47 CFR 1.1206, 1.1203. To be clear, while the Commission recognizes that consultation with these entities is critically important, the Commission will rely in its decision-making only on facts and arguments that are placed in the public record for this proceeding. To this end, the enumerated Federal Government entities, like all interested parties, should submit in the public record of this proceeding comments, reply comments, and other presentations presenting those facts and arguments they wish the Commission to rely on in its decision-making process. If the presentation made by staff of one of the federal agencies enumerated above is of ''substantial significance and clearly intended to affect the ultimate decision,'' the Commission will rely on such presented information in its decision-making process only if it coordinates in advance with the agency involved to ensure that such agency retains control over the timing and extent of any disclosure that may impact that agency's jurisdictional responsibilities. *See* 47 CFR 1.1206(b)(3).

Paperwork Reduction Act: This document may contain proposed modified information collection requirements. Therefore, the Commission seeks comment on potential new or revised information collections subject to the Paperwork Reduction Act of 1995. If the Commission adopts any new or revised information collection requirements, the Commission will publish a notice in the **Federal Register** inviting the general public and the Office of Management and Budget to comment on the information collection requirements, as required by the Paperwork Reduction Act of 1995, Public Law 104–13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, see 44 U.S.C. 3506(c)(4), the Commission seeks specific comments on how it might further reduce the information collection burden for small business concerns with fewer than 25 employees.

Regulatory Flexibility Act: The Regulatory Flexibility Act of 1980, as amended (RFA), requires an agency to prepare a regulatory flexibility analysis for notice-and-comment rulemakings, unless the agency certifies that ''the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities.'' The Commission seeks comment on potential rule and policy changes contained in the document, and accordingly, has prepared an IRFA. The IRFA for this document in PS Docket Nos. 24–146 and 22–90 is set forth below in this document and written public comments are requested. Comments must be filed by the deadlines for comments on the *NPRM* indicated under the **DATES** section of this document and must have a separate and distinct heading designating them as responses to the IRFA. The Commission reminds commenters to file in the appropriate dockets: PS Docket Nos. 24–146 and 22–90.

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

Synopsis

Introduction and Background

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

2. As of May 2024, only 38% of U.S. networks allow for the validation of their routing information by registering and maintaining ROAs in the RPKI. That figure is derived from data found in Cloudflare's Radar, and it is confirmed by data in the MANRS Observatory. The MANRS Observatory provides trend data for the maintenance of routing information in the RPKI by the networks participating in MANRS. There are other measurement tools publicly available online that reveal similar data, such as NIST's RPKI Monitor. Looking at an earlier date, as of December 2024, 36% of traffic originating from non-U.S. Federal Government networks was covered by a valid ROA, but less than 1% of traffic originating from U.S. Federal Government networks was covered by a valid ROA. Thus, we observe that the use of RPKI services across the internet has continued to increase over the past several years through service providers seeking to secure their BGP architectures. Despite the increasing deployment of RPKI-based security measures by some service providers in the United States, service providers that participate in BGP routing will need to make additional progress to reduce exposure to the types of communications attacks described and the ensuing risks.

3. Thus, consistent with comments filed by DOD, DOJ, and CISA in response to the *Secure internet Routing NOI,* we are proposing reporting obligations on service providers intended to help assess, prioritize, and maintain plans for utilizing the RPKI architecture to further BGP operational security. As the agency with regulatory authority in this area, we intend to continue our close collaboration with

other federal agencies which have been actively considering similar secure internet routing issues through National Cybersecurity Strategy initiatives. We seek comment on how the deployment of RPKI and other solutions may promote accountability through collaboration among key internet stakeholders, such as private, government, regulated, and unregulated entities, and between the United States and our global partners. Our proposals are largely focused on the preparation and filing of BGP Routing Security Risk Management Plans, but we do seek comment on certain additional measures that we believe hold promise for facilitating the implementation of RPKI-based routing security.

A. BGP Routing Security Risk Management Plans

4. We propose to require service providers to prepare and maintain BGP Routing Security Risk Management Plans (BGP Plans) describing and attesting to the specific efforts they have made, and further plan to undertake, to create and maintain ROAs in the RPKI. We expect that requiring service providers to prepare plans on how they have and will institute RPKI, a solution developed through an open standards setting process, can promote participation in the standards setting process. The Commission continues to strongly support open standards setting processes, and that is also a core goal of strategic objective 4.1 of the National Cybersecurity Strategy. We seek comment on the impact that our reporting proposals may have on this goal.

5. Under our proposals, BGP Plans can be risk-based performance plans, but would have to describe and attest to the extent to which the service provider conducts ROV filtering at the interconnection points between the service provider and its peers and clients, as well as describe any other methods at their disposal. These plans are to be updated on an annual basis. The following subsections discuss which service providers would be required to confidentially file their BGP Plans with the Commission, in addition to discussing the details that we propose should be included in all BGP Plans, whether filed with the Commission or not. Should the Commission promote risk-based solutions among service providers?

1. Initial BGP Plans

6. We propose to require certain large service providers to file initial BGP Plans with the Commission. In particular, we propose to impose this filing requirement on all Tier 1 service providers as well as the other most significant service providers, which would currently include: AT&T, Inc.; Altice USA; Charter Communications; Comcast Corporation; Cox Communications, Inc.; Lumen Technologies, Inc.; T-Mobile USA, Inc.; Telephone & Data Systems (including US Cellular); and Verizon Communications, Inc. These significant providers are likely to originate routes covering a large proportion of the IP address space in the United States and will play critical roles ensuring effective implementation of ROV filtering. The initial BGP plans prepared by service providers other than those suggested above would not need to be filed with the Commission but should be made available to FCC staff upon request. We propose, but seek comment on, a requirement that BGP Plans submitted to the Commission should be attested by a corporate officer at each service provider.

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

8. We do not propose in this *NPRM* to set specific industry-wide substantive requirements with industry-wide deadlines. BGP Plans are intended to establish a mechanism by which the Commission, working in coordination with other federal agencies, can assess a service provider's actions to prioritize routing security through use of the RPKI architecture, measure its progress over time to evaluate the reasonableness of its BGP routing security risk management plan, and verify its commitments to following it. In addition, the development of BGP Plans by all service providers would be important for securing BGP operations in the near term because it would require service providers to consider the benefits of creating and maintaining ROAs and conducting ROV filtering. We recognize that service providers often have different network architectures and different technologies, partly as a reflection of the types of customers and services offered, and that these differences may have affected the speed with which they have deployed RPKI and may affect their plans going forward. We seek comment on whether our proposals address these issues and promote the implementation of routing security among U.S. service providers. The specific BGP Plan requirements concerning ROAs and ROV are discussed *seriatim.* We seek comment generally on whether it would be helpful for the Public Safety and Homeland Security Bureau (PSHSB) to develop a standardized template for preparing BGP Plans. We also seek comment on how service providers should respond if mandatory elements of a BGP Plan do not apply to their particular circumstances.

a. Creating and Maintaining Route Origin Authorizations

9. Registering and maintaining updated ROAs with the appropriate internet registry is a critical and necessary step for securing BGP operation in the near term. At present, only the holders of specific IP address prefixes can register ROAs for originated routes that pertain to those prefixes. As a result, a service provider is able to directly register and manage ROAs only when it controls the IP address prefix(es) in question. An effective path forward must therefore take into account the difference in the service provider's route origination control over the IP prefix(es) assigned to it by ARIN. The information we would require service providers to submit would depend on the various categories of IP address prefixes for which a service provider can be the route originator. In the subsections below, we discuss the different cases that we have observed in which the service provider either does or does not control the IP address prefix(es) assigned or allocated to it and route originations for the same. We anticipate that most service providers will be originating routes for prefixes drawn from all these cases. We would evaluate RPKI deployment in each set of circumstances differently depending on what type of control the service provider has over route originations to various IP address prefix(es).

i. Cases Where the Service Provider Controls the ASNs and IP Address Prefix(es)

10. We first consider where a service provider has full authority to register ROAs because it controls the associated IP address prefix(es). ROAs are registered with the responsible regional registry, which is ARIN for the United States and North America. ARIN assigns

ASNs and IP address prefixes to the Local Internet Registries (LIRs). As set out in the ARIN Manual, LIRs are ''generally ISPs whose customers are primarily end users and possibly other ISPs.'' The ISP might in turn designate a subset of the IP address space it holds to be used by its customers, but in the current ARIN operational convention only the original ISP can register ROAs even for reallocated address space.

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

12. We seek comment on the criteria by which we should evaluate the relevance of individual BGP Plans filed with, or reviewed by, the Commission. We recognize, for instance, that different service providers are in substantially different positions regarding the extent to which they control the ASN and the IP address prefixes that they originate. We also understand that some service providers have fewer in-house resources available than others. We recognize as well that the processes for creating ROAs for legacy number resources originally issued to the service provider by an Internet Registry prior to the creation of ARIN may raise additional issues, and we seek comment on how our proposals may address those issues. Finally, we anticipate receiving detailed explanations if a service provider contends that ''multi-homing,'' traffic engineering, or some other factor significantly reduces its ability to increase and maintain ROA coverage for IP prefixes they control. Regarding multi-homing, are there measures that would facilitate coordinating all necessary ROAs for all the ASNs that may originate routes to the same prefix? What are factors that might inhibit such coordination? If at least one ROA registration of the IP prefix is valid, is that sufficient to protect the IP prefix even if there are other invalid registrations for that prefix?

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

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

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

15. For these cases, we propose to require that a service provider's initial BGP Plan describe the status of the ROA registrations for routes they originate within these three cases. We propose that the BGP Plan explain the reason(s) why the service provider is unable to register particular sets of IP prefixes. The Plan should also describe in detail the service provider's efforts and plans for facilitating the ROA registrations for the IP prefixes that have been transferred and not under its control. Among other issues, we believe that BGP Plans would need to describe the steps that the service provider takes to identify and address cases in which customers or clients with their own IP prefixes are multi-homed and the frequency it encounters multi-homing. In multi-homing situations where it is the responsibility of the customer or client to create and register, rather than the service provider, the chances for errors in ROA registration may be greater, potentially resulting in the customer's traffic becoming blackholed through a given provider. We understand that in many cases, the service provider will have direct contractual relationships with the holder of the IP address prefixes and will be, or can be, made aware of the ROA registration status of those prefixes with ARIN. Although the service provider itself is not able at this time to register ROAs in these circumstances, we are seeking comment on the steps that service providers can or should do to help secure ROAs for the IP address space held by downstream clients.

b. Route Origin Validation Filtering

16. The implementation of ROV is necessary to determine whether received route advertisements are legitimate when checked against ROAs in the RPKI repositories. ROV is the step in origin validation predicated on the existence of ROAs, and is the key action that facilitates detection of invalid or unknown route originations that indicate a prefix is being incorrectly advertised, either maliciously or accidentally, by a service provider or enterprise network. For the RPKI to be effective, most if not all service providers will need either to conduct ROV filtering in their interconnections

with other service providers, or to have contractual commitments with third parties to have routes propagated to them subject to ROV filtering. Moreover, to fully realize the origin validation benefits of the RPKI, some service providers may need to perform ROV filtering in interconnections with their clients. In this way, the service provider examines incoming BGP routing announcements from its peers in addition to its clients. In cases where a service provider is downstream from a more widely accessed provider (*e.g.,* stub networks), there could be great benefits from the downstream provider relying on the ROV filtering performed by its upstream provider.

17. We propose that the BGP Plan of a Tier 1 service provider should describe the extent to which it has implemented ROV filtering at its interconnection points with its peers as well as its customers, and to what extent ROV has been disabled or not deployed within its network. We also propose that BGP Plans describe, to the extent applicable, any contractual requirements a service provider may have for upstream third-parties to provide ROV filtering for incoming routes. We seek comment on whether this information would be required of all BGP Plans, whether filed with the Commission or made available upon request. We believe that this information is likely to be most relevant for Tier 3 service providers who do not have peering relationships and solely rely on contracts with other upstream service providers. We seek comment on the use of this information to monitor the effective deployment of ROV.

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

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

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

2. Subsequent BGP Plans

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

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

23. We also seek comment on the content that needs to be included in the BGP Plans prepared after the initial Plans. We anticipate that subsequent Plans would largely consist of updates to the initial Plans, so that the burden of preparing such Plans would be significantly less than preparing the initial Plans. We seek comment on that conclusion and on what information should be included in subsequent Plans. We seek comment on when the requirement to prepare subsequent BGP Plans annually should sunset, such as in five years. Would the information included in these plans become less important as the RPKI is extensively deployed? To that end, we seek comment on the frequency with which the Commission should revisit the form and content of BGP Plans.

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

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

generally take into account the different circumstances of various service providers.

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

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

B. BGP Routing Security Information—Quarterly Reports

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

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

29. As noted above, there may be special challenges in the cases of ROAs for routes pertaining to networks that are multi-homed, and so the prevalence of such routes may well be relevant in assessing the security of the BGP routing system. To what extent are service providers aware of multi-homing scenarios for the routes they originate, and can they enumerate and report on these use cases? Are there other sources of information on these cases? We believe that quarterly reporting is necessary, at least initially, to measure on a reasonably timely basis the evolution of RPKI-derived routing security, and to determine whether additional steps are needed—whether regulatory or otherwise—to encourage continued progress. We also believe that the data proposed for collection should be readily available within the individual service providers. In addition, once collected, it should not be burdensome to be updated on a quarterly basis. For instance, ARIN repositories are updated every five minutes, and the NIST RPKI Monitor updates its analyses every six hours to reflect the corresponding route collector updates. We seek comment as to whether the reporting obligations in this context should be reduced if a service provider files with the Commission an attestation that—as specified above with regard to subsequent BGP Plans—it has achieved and maintained ROAs covering at least 90% of originated routes in IP address prefixes that it controls. In those cases, would semi-annual or annual reporting be sufficient for monitoring that service provider's progress toward full RPKI implementation? Would any data reporting be necessary? We seek comment on this approach.

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

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

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

C. Confidential Treatment of BGP Plans and FOIA

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

D. Other Issues

1. Possible Conditions on Service Provider Contracts

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

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

36. For instance, from our continuing stakeholder engagement, we understand that service providers believe that they are not in a position to insist in these situations that client customers register ROAs for these IP address prefixes. Unlike some internet participants that have successfully adopted policies that require ROA registration for interconnection, service providers believe that they are not in a position to adopt similar policies and practices because client customers are likely to have alternative options for their upstream service provider who would not insist that the IP address holder take the additional step of registering ROAs.

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

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

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

40. Again, we seek to address any potential for collective action issues under these circumstances. Would a service provider or its customer be likely to encounter any disincentives for the registration of ROAs, particularly if, in the absence of any conditions, other service providers are free not to do so? We seek comment on the likelihood that

a service provider might lose customers if it wanted to require ROA registration (and/or ROV filtering) to be implemented by their peering or downstream neighbor. Assuming that a peering or downstream service provider (*e.g.,* Tier 3 provider) might well choose a different transit provider to connect their customers to the internet if the alternate transit provider did not require the downstream service provider to register and maintain accurate ROA objects pertaining to its IP address prefixes, to what extent can providers of transit or other interconnectivity services incorporate mandatory language into the corresponding contractual agreements?

41. To address these potential collective action barriers to widespread ROA registration, we seek comment on requiring that providers' contracts in these cases to provide for the registration of ROAs for the relevant IP address prefixes. For instance, as identified above, we seek comment on requiring service providers not to enter into new contracts to route traffic unless ROAs are registered for the relevant IP address prefixes. Should such contracts also require the holder of the IP prefix to maintain the active ROAs? We also seek comment on requiring service providers to mandate that clients with whom they have a direct contractual relationship to register their IP prefixes with ARIN. If a client refuses to register assigned prefixes, could a service provider ''take back'' unregistered IP address prefixes it has leased to others so as to enable the service provider to register ROAs for those prefixes? We recognize possible disruptions in certain cases that may outweigh the benefits, and so seek comment on imposing certain requirements at the time of contract renewal. In order to judge the potential benefits and costs of any such requirements, we seek comment on whether general industry standards exist for setting the term of any such contracts. We also recognize that any such requirement would depend on the provisions and terms of the existing contracts, as well as when their contracts are set to renew. We further seek comment on the percentage of client contracts that extend beyond two years of the publication of this proceeding. For instance, if a substantial percentage of contracts are five years or longer, should the Commission consider imposing requirements no later than a set time period, such as two years from the effective date of the adoption of rules.

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

2. Possible ROV and ROA Requirements for Service Providers

43. We have sought comment above on whether the ROV implementation content of the BGP Plans of Tier 1 and Tier 2 service providers should differ depending on whether they are able to attest to certain ROV implementation. We here seek comment on proposals to require certain levels of implementation of ROV by Tier 1 and Tier 2 service providers. In particular, we seek comment on whether Tier 1 service providers should be required to achieve the ROV deployment described above within one year of the effective date of such a requirement, and whether Tier 2 service providers should be required to achieve the ROV deployment described above within two years of the effective date. As described above, ROV implementation is a critical piece of successful RPKI implementation, and we believe that those target dates are reasonable given the current state of ROV deployment. We seek comment on whether ROV implementation requirements would be consistent with the Commission's expressed construction of the proposals contained in this *NPRM* to establish a framework for multistakeholder collaboration instead of a rigid regulatory mandate.

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

3. Outreach and Education

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

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

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

4. ARIN Processes

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

5. Beyond RPKI Origin Validation—Further Efforts To Secure Internet Routing

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

Appendix A

Technical Appendix: Additional Background on Inter-Domain Routing

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

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

3. The networks interconnected by BGP are termed BGP Autonomous Systems (ASes) and are referred to by their Autonomous System Numbers (ASNs). An AS may include one or multiple separate networks, collectively all under the technical administration of a single entity. For BGP purposes, a network path is denoted as a string of ASNs termed an AS Path. The AS Path is one of the ''BGP path attributes'' or control variables used in signaling BGP reachability that influences how each BGP speaker selects routes to a specific destination. Originally, the AS Path was intended to reflect the initial ASN originating an advertisement for a prefix, as well as the succession of ASes traversed by a BGP update (the basic BGP message carrying signaling information). However, no means were provided to verify whether this attribute was correct or false in any way. Deliberations on how best to address this type of risk and others have occurred since at least 1997. As these and other references cited note, there are additional vulnerabilities that go beyond the ones described in this section.

4. A BGP route can be defined as a destination prefix associated with a string of BGP Path attributes. Attributes provide the semantics that affect how the BGP logic in each BGP speaker processes the routes it receives from other BGP speakers. The BGP hijacks referred to in this document deal with

incidents associated with manipulating the AS Path attribute, including distorting or falsifying the Origin AS, or the originated route specificity. Some of the relatively more well-known routing incidents have involved these attack vectors.

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

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

Federal Communications Commission.

Marlene Dortch,

Secretary.

[FR Doc. 2024–13048 Filed 6–14–24; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 90 and 95

[ET Docket No. 19–138, DA 24–538; FR ID 225149]

Use of the 5.850–5.925 GHz Band

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Office of Engineering and Technology invites supplemental comment to address issues regarding the use of geofencing in cellular-vehicle-to-everything on-board units to reduce out-of-band emission power limits around specified federal radiolocation services.

DATES: Interested parties may file comments on or before July 5, 2024.

ADDRESSES: Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR 1.415, 1.419, interested parties may file comments on or before the dates provided in the ''Dates'' section of this Proposed Rule. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). You may submit comments, identified by ET Docket No. 19–138 and referencing this public notice, by any of the following methods:

- *Electronic Filers:* Comments may be filed electronically using the internet by accessing the ECFS: *https://www.fcc.gov/ecfs/.*
- *Paper Filers:* Parties who choose to file by paper must file an original and one copy of each filing.
- Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by First-Class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
- All hand-delivered or messenger-delivered paper filings for the Commission's Secretary are accepted between 8:00 a.m. and 4:00 p.m. at 9050 Junction Drive, Annapolis Junction, MD 20701. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
- Commercial overnight deliveries (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 Secretary, Federal Communications Commission, 45 L Street NE, Washington, DC 20554.
- *People with Disabilities:* Contact the Commission to request reasonable accommodations (accessible format documents, sign language interpreters, CART, etc.) by email: *FCC504@fcc.gov* or phone: 202–418–0530 or TTY: 202–418–0432.
- *Availability of Documents:* Comments and *ex parte* submissions will be available via ECFS. Documents will be available electronically in ASCII, Microsoft Word, and/or Adobe Acrobat.

FOR FURTHER INFORMATION CONTACT: Brian Butler of the Office of Engineering and Technology, at *Brian.Butler@fcc.gov* or 202–418–2702.

SUPPLEMENTARY INFORMATION: This is a summary of the Office of Engineering and Technology's Public Notice in ET Docket No. 19–138, DA 24–538, released June 11, 2024. The full text of this document is available for public inspection at the following internet address: *https://www.fcc.gov/document/oet-seeks-comment-board-unit-power-limits-c-v2x-operations.*

Regulatory Flexibility Analysis. The *Further Notice of Proposed Rulemaking* (*FNPRM*) in ET Docket No. 19–138 included an Initial Regulatory Flexibility Analysis (''IRFA'') pursuant to 5 U.S.C. 603, exploring the potential impact on small entities of the Commission's proposals. *Use of the 5.850–5.925 GHz Band,* 86 FR 23323, 23333–36 (May 3, 2021). We invite parties to file supplemental comments on the IRFA in light of this request to refresh the record.

Paperwork Reduction Act Analysis. This document does not contain any new or modified information collection requirements subject to the Paperwork Reduction Act of 1995, Public Law 104–13. Thus, it does not contain any new or modified information collection burden for small business concerns with fewer than 25 employees, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, see 44 U.S.C. 3506(c)(4).

Ex Parte Presentations. This proceeding shall be treated as ''permit-but-disclose'' in accordance with the Commission's *ex parte* rules. 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)