ROADMAP TO ENHANCING INTERNET ROUTING SECURITY

A REPORT BY THE WHITE HOUSE
OFFICE OF THE NATIONAL CYBER DIRECTOR

SEPTEMBER 2024

THE WHITE HOUSE
WASHINGTON

Table of Contents

Introduction

A secure and open Internet is critical to the economic prosperity and national security of the United States. However, many aspects of the Internet's architecture and ecosystem, including the principal technology used to route traffic across the thousands of independent networks that comprise the Internet, do not provide adequate security for the threats we face today. A strategic objective of the National Cybersecurity Strategy[1] is to secure the technical foundation of the Internet. To increase the resilience of Internet routing and the broader digital ecosystem, the 2023 National Cybersecurity Strategy Implementation Plan states:

> **The Office of the National Cyber Director, in conjunction with key stakeholders and appropriate Federal Government entities, will develop a roadmap to increase the adoption of secure Internet routing techniques and technology by: (1) identifying security challenges; (2) exploring approaches and options to address Internet routing and [Border Gateway Protocol] BGP security concerns; (3) identifying and informing the development of best practices; (4) identifying needed research and development; and (5) identifying barriers to adoption and alternative mitigation approaches.[2]**

To that end, this document serves as a roadmap to increase the adoption of technologies that address critical vulnerabilities associated with the Border Gateway Protocol (BGP) and drive improvements in Internet inter-domain routing security and resilience. This roadmap is not a technical guide on how to implement routing, but rather points to best-available guidance and practices, details United States Government (USG) actions to promote BGP security, and makes recommendations to improve routing security throughout the Internet ecosystem.

Overview of the Complexity and Risks in Internet Routing

The Internet comprises approximately 74,000 independently operated but interconnected networks called Autonomous Systems (ASes).[3] These networks are quite diverse in terms of their purpose, business models, clients served, geographic size, speed, number of attached devices, and internal network technologies. Examples include residential broadband, business and critical infrastructure enterprise, mobile wireless, cloud service, content distribution, operational technology, and Internet transit networks.

---

[1] *The National Cybersecurity Strategy*, The White House, July 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[2] *The National Cybersecurity Strategy Implementation Plan*, The White House, July 2023, 38, https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.
[3] *See* "The 32-bit AS Number Report," https://www.potaroo.net/tools/asn32/.

One thing that all these networks have in common is the use of BGP to dynamically exchange routing information with other ASes to which they connect. BGP is typically used by *border routers* that directly connect with routers in another network operated by a different organization.[4] These routers use BGP to announce destination addresses (i.e., aggregated representations of network address blocks expressed as "address prefixes") that they can reach directly, as well as the destinations they can reach through neighboring networks, and to receive announcements from neighboring networks of feasible paths toward more remote destinations.

In addition to destination address prefixes, BGP announcements must include an attribute documenting the Internet route to each destination encoded as the sequence of other networks (i.e., AS path) that traffic to the destination would cross. Additional optional attributes may encode information about the business relationship of the neighbor that announced the route (e.g., customer, provider, or peer networks) and policy information that can be used to limit how the learned route can be shared with other neighboring networks. BGP routers select the "best path" to each destination address prefix from the routes advertised by their neighbors. This best path determines the neighboring network to use when forwarding data traffic toward each unique destination on the Internet. The policy used to select the best path to each destination is entirely local to each network, but it is typically based on preferred routes learned from customer networks or routes with shorter AS paths.

The topology of the global Internet (i.e., which ASes are directly interconnected and which destinations are directly reachable by each AS) is vast and constantly evolving. This evolution occurs due to business decisions that result in networks adding or dropping BGP neighbors; operational decisions as networks change their best path selections; or by circumstance, such as network interconnections failing or paths to destinations changing. In today's Internet, a BGP router can receive announcements for more than one million unique address prefixes,[5] often with multiple disjoint paths to reach each destination.

As initially designed and commonly operating today, BGP does not provide adequate security and resilience features for the risks we currently face. Concerns about fundamental vulnerabilities have been expressed for more than 25 years. BGP's design lacks the capability to:

- Validate the authority of remote networks to originate announcements to specific destinations;
- Verify the integrity and authenticity of messages exchanged between neighboring networks;
- Ensure the authenticity and integrity of information from remote networks; and
- Detect routing announcements that violate business policies between neighboring networks.[6]

[4] While BGP is used in several other contexts in modern information systems, this roadmap is limited to the use of BGP for inter-domain routing.
[5] *See* "NIST RPKI Monitor," NIST, Version 2.0, https://rpki-monitor.antd.nist.gov/.
[6] Sandra L. Murphy, *RFC 4272: BGP Security Vulnerabilities Analysis*, Internet Engineering Task Force, January 2006, https://datatracker.ietf.org/doc/rfc4272.

★ ★ ★ ★ ★ ★

As the Internet grew in scale and complexity, the lack of these capabilities often led to accidental misconfigurations that resulted in widescale impacts on Internet routing.[7] As the Internet became essential to global commerce, critical infrastructure, and communications, malicious actors began purposefully exploiting these BGP vulnerabilities. Attackers began to falsify BGP information to cause data to be delivered to the wrong destinations, to divert paths across the Internet to pass through unintended networks, or to cause outages in Internet connectivity. Such incidents are generally called route hijacks because the action of a third party results in disruptive and often damaging changes in the routing of Internet traffic.

Route hijacks can expose personal information; enable theft, extortion, and state-level espionage; disrupt security-critical transactions; and disrupt critical infrastructure operations.[8] While most BGP incidents are accidental, the concern over malicious actors has elevated this issue to a national security priority.

In recent years, there have been numerous incidents involving BGP routing anomalies, such as:

- *Prefix hijacks*—networks originating false or unauthorized announcements of destination addresses to cause misdelivery of Internet traffic.
- *Path hijacks*—networks improperly modifying BGP attributes, such as the AS path, to divert traffic along unintended Internet routes.
- *Route leaks*—networks improperly announcing routes that violate business policies between networks, often resulting in large-scale routing outages.[9]

There is growing evidence of sophisticated attacks that purposefully manipulate BGP to subvert other foundational protocols, such as the Domain Name System (DNS), web public key infrastructure, and end-to-end security protocols. These malicious attacks exploited known BGP vulnerabilities to enable cryptocurrency theft and malware distribution, and compromise privacy or censor individual communications.[10] In 2022, the Cybersecurity and Infrastructure Security Agency (CISA) noted foreign adversaries' willingness to exploit BGP vulnerabilities.[11]

The Need for Increased Action

Improving the security and resilience of Internet routing is a challenging task. BGP is a single, globally-deployed protocol that must remain continuously interoperable across tens of thousands of independent networks. No single technical approach will solve all Internet routing vulnerabilities, nor are all threats confined to those described above.

Improving Internet routing security will require action by network operators, including Internet service providers (ISPs), mobile network operators, cloud service providers, content distribution

[7] *Security of the Internet's Routing Infrastructure*, Broadband Internet Technical Advisory Group, November 2, 2022, https://www.bitag.org/Routing_Security.php.
[8] See *Cybersecurity Framework Profile for Internet Routing*, CableLabs Security, January 23, 2024, 7, https://www.cablelabs.com/specifications/CL-GL-RS-Profile.
[9] Kotikalapudi Sriram et al., *RFC 7908: Problem Definition and Classification of BGP Route Leaks*, Internet Engineering Task Force, June 2016, https://datatracker.ietf.org/doc/rfc7908/.
[10] *Security of the Internet's Routing Infrastructure*, Broadband Internet Technical Advisory Group.
[11] *In the Matter of Secure Internet Routing*, PS Docket No. 22-90, Reply Comments of the Cybersecurity and Infrastructure Security Agency, FCC 22-18, June 28, 2022, https://www.fcc.gov/ecfs/document/10707962804139/2.

networks, critical infrastructure networks, and enterprise networks of all types, such as commercial, academic, and Federal, state, local, Tribal, and territorial (SLTT) governments. Technical solutions will require collective action among edge networks (i.e., enterprise, user, cloud, and content networks) and transit networks.

Initial techniques to improve the security and resilience of BGP have been standardized, are commercially available, and are being deployed at varying levels in different regions and industry sectors of the Internet. This roadmap provides recommendations and guidance necessary to increase the adoption of these initial BGP security technologies across all network operators in the Internet ecosystem.

Baseline Approaches to Address BGP Vulnerabilities

A decade of work by the Internet Engineering Task Force (IETF), Regional Internet Registries (RIRs),[12] and vendor and network operator communities has resulted in the design, standardization, and commercial availability of technologies to address some of the most common BGP vulnerabilities. While work continues within the IETF and broader Internet technical community to develop additional BGP security mechanisms, this roadmap focuses on the baseline actions that all network operators should take at the earliest practical opportunity to adopt mature, standardized technologies readily available today.[13]

The technical basis for many current and emerging BGP security mechanisms is the Resource Public Key Infrastructure (RPKI). RPKI is a global trust infrastructure developed specifically to enable new BGP security mechanisms.[14] The RIRs act as RPKI certificate authorities (CAs) that issue digital certificates to organizations that identify the Internet Protocol (IP) address blocks and AS numbers they have been allocated. AS and address holders use these certificates to digitally sign data objects that third parties can validate for authenticity and integrity. These certificates and digitally-signed objects are published in distributed RPKI repositories. Each of the five RIRs provide RPKI services; in North America, the RIR is the American Registry for Internet Numbers (ARIN).[15]

Current Best Practice: RPKI, ROA, and ROV

Route Origin Validation (ROV) is the first RPKI-based BGP security mechanism to become widely and commercially available. As noted, one fundamental vulnerability in BGP's design is the lack of mechanisms to verify which networks were authorized to announce specific address

[12] "Regional Internet Registries," The Number Resource Organization, https://www.nro.net/about/rirs/.
[13] Many other mechanisms to address some aspects of BGP vulnerabilities have been used in the Internet for some time (e.g., Internet Routing Registries). Such techniques are well documented in existing guidance. This roadmap does not attempt to replicate that guidance.
[14] *See* M. Lepinski and S. Kent, *RFC 6480: An Infrastructure to Support Secure Internet Routing*," Internet Engineering Task Force, February 2012, https://datatracker.ietf.org/doc/html/rfc6480.
[15] "Resource Certification (RPKI)," ARIN, https://www.arin.net/resources/manage/rpki/.

blocks as being directly reachable through them. ROV,[16] based on Route Origin Authorization (ROA)[17] data, was designed to address this vulnerability. The RPKI security mechanism is comprised of two components:

- ROAs are data objects created by the holders of address blocks declaring which networks are authorized to originate[18] specific address prefixes from those blocks in BGP.
    - ROAs are digitally signed using the RPKI certificates issued to the address holders and are published in RPKI repositories.
- ROV is the process by which BGP routers use ROA data to filter received BGP announcements flagged as invalid either because of their origin AS or prefix length.
    - The common implementation of ROV uses *RPKI-validating cache servers* to gather global RPKI data, perform cryptographic validation of the digitally-signed objects, and transmit a highly simplified version of the validated ROA data to BGP routers.[19]
    - BGP routers use this distilled ROA data to classify the prefix and origin of each received BGP route as either valid, invalid, or not found.[20]
    - Network operators implementing ROV configure local BGP policies based on the ROV result. The suggested BGP policy is to mark ROV-invalid routes as ineligible to be selected as the best path for forwarding data traffic.[21]

Today, the standards, infrastructure services, and commercial products necessary to adopt and deploy ROAs and ROV are readily available.

- The IETF standards for RPKI services, ROA creation and validation, and ROV processing in BGP routers are mature and well-tested. Many organizations have developed best common-practice guidance that documents how to incrementally adopt RPKI and ROV in production networks.[22]
- All five RIRs offer production RPKI services for issuing certificates and facilitating the creation and publication of ROAs. The RIRs offer these services in a *hosted model* where the RIR handles all of the certificate management, ROA creation, repository publication tasks, and RPKI operations on its servers. RPKI services, such as ROA creation, are

[16] We use the term ROV to mean Route Origin Validation based on RPKI ROA data. While other methods and data sets may perform similar functions, in this document, ROV refers specifically to the methods described in P. Mohapatra, et al., *RFC 6811: BGP Prefix Origin Validation*, Internet Engineering Task Force, January 2013, https://datatracker.ietf.org/doc/html/rfc6811.
[17] We use the term ROA to refer to RPKI-based route origin authorization and the ROA data objects created and published in the RPKI.
[18] A network that announces a prefix as being directly reachable is referred to as the *origin AS* and such announcements are referred to as *BGP originations*.
[19] A key attribute of this implementation architecture is that it does not require any cryptographic operations to be performed on the routers.
[20] ROV was designed for incremental adoption. The ROV result of "not found" is returned when ROA data for a given BGP announced prefix has not been created.
[21] This policy is commonly referred to as "filtering," "ignoring," or "dropping" invalid routes.
[22] Kotikalapudi Sriram and Doug Montgomery, *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*, NIST SP 800-189, December 2019, and https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189.pdf; "Resource Public Key Infrastructure (RPKI) FAQs & Best Practices," ARIN, https://www.arin.net/resources/manage/rpki/faq/.

typically accessible through a web interface and network application programming interfaces for automation.

    - Most RIRs also support a *delegated model* in which in which the network operator provides some or all of these RPKI services for its assigned resources (e.g., signs route origin authorizations, issues subordinate resource certificates to its customers, etc.).[23]

- Multiple implementations of RPKI-validating caches exist and are deployed in production networks.[24]

Most commercial router implementations support the ability to perform ROV based on ROA data. Over the last five years, the adoption of RPKI, ROA, and ROV in some regions of the Internet has been significant. In Europe, approximately 70% of BGP routes originated have published ROAs and are ROV-valid.[25] However, adoption rates are significantly lower in North America (i.e., the ARIN region) and specific industry sectors. The following sections explore and explain why adoption may lag in the ARIN region and offer a plan of action to improve the situation.

Challenges to RPKI Adoption

In the regions of the Internet and industry sectors where adoption of BGP security technologies is lagging, there are three common contributing factors. One, decision-makers lack a thorough understanding of Internet routing security risks and the readily-available technologies to mitigate them. Two, network operators face competing engineering priorities, misaligned incentives, and limited resources to deploy new BGP security mechanisms. Three, organizations planning to adopt RPKI-based technologies may encounter administrative barriers when attempting to contract with their RIR. Each of these challenges can contribute to a general reluctance to prioritize routing security despite its foundational importance to the Internet ecosystem.

Prioritization, Resourcing, and Perceived Risk

BGP's insecurity has the potential to impact the entire Internet ecosystem, affecting service providers of all types, enterprises and organizations of all sizes (including large corporations, schools, libraries, hospitals, banks, emergency services, utilities, small businesses, the public at large, and government organizations), and individual users.

The adverse impacts and costs of BGP insecurity are often not directly felt by the network operators responsible for implementing BGP security protocols. Investing in network security may not provide an apparent near-term competitive advantage or a clear return on investment, reducing market incentives to invest.[26] As a result, network operators may view routing security

[23]. Kotikalapudi Sriram and Doug Montgomery, NIST SP 800-189.
[24] *See* "RPKI: Software Projects," NLnet Labs, https://rpki.readthedocs.io/en/latest/ops/tools.html.
[25] *See* "NIST RPKI Monitor."
[26] *Routing Security for Policy Makers*, Internet Society, October 2018, https://www.internetsociety.org/wp-content/uploads/2018/10/Routing-Security-for-Policymakers-EN.pdf; *Routing Security: BGP Incidents, Mitigation Techniques and Policy Actions*, OECD Digital Economy Papers, No. 330, October 2022, 33, https://www.oecd.org/publications/routing-security-40be69c8-en.htm.

as important, but prioritize it below other competing cybersecurity concerns. Routing security sometimes gets overshadowed by more visible priorities.

Some network service providers have indicated that many of their customers do not understand how implementing routing security will benefit them. Internet stakeholders have noted that implementing RPKI competes for attention, funding, and personnel with other high-priority business and cybersecurity needs. There are also resourcing constraints to consider, as some operators noted that some of their deployed equipment, such as their routers, are incapable of performing ROV and would need to be replaced to implement these functions. More generally, many network operators hesitate to adopt new or unfamiliar technology because of the concern of potential service disruptions to their customers.

The USG identified the need to secure the technical foundation of the Internet as critical to ensuring a resilient digital ecosystem.[27] BGP insecurity poses real, systemic vulnerabilities that can be exploited by foreign adversaries and criminal actors to conduct malicious activity and threatens U.S. personal data and the integrity of U.S. telecommunications networks. The mitigation of these risks should be appropriately prioritized.[28] RPKI, ROA, and ROV offer network operators a commercially-viable approach to address some of this risk and attain a higher level of security.

Administrative Barriers

Organizational and administrative barriers can hamper Internet routing security. These include a lack of situational awareness regarding an organization's existing Internet address resources and route origination status, unclear authority for implementing security measures, and a lack of coordination across teams to achieve more secure routing. Organizations may have acquired their Internet address blocks many years ago, prior to the arrival of current staff who are responsible for managing these allocations. Additionally, mergers and acquisitions may have led to accounting challenges for managing Internet address resources. However, inadequate management of address resources should not be accepted as an excuse for inefficient network operation and the failure to implement routing security. The address space of any network is a valuable resource critical to efficient and secure operation.

Barriers also flow from legal considerations. Administrative barriers and potentially problematic contract provisions in RIRs' registration service agreements (RSAs) may play a role in stunting RPKI implementation among holders of "Legacy"[29] Internet address resources, including the USG. For example, the USG is not able to accept the standard RSA provisions regarding bankruptcy, indemnification, and governing law and venue.[30]

---

[27] *The National Cybersecurity Strategy*, The White House, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[28] *See* U.S. Department of Justice and U.S. Department of Defense to Federal Communications Commission, *Re: In the Matter of Secure Internet Routing*, PS Docket 22-90, September 14, 2022, https://www.fcc.gov/ecfs/document/1091496862125/1.
[29] "Legacy" means IP resources that were held before ARIN was established in 1997.
[30] Christopher S. Yoo and David A. Wishnick, "Lowering Legal Barriers to RPKI Adoption," January 8, 2018, https://scholarship.law.upenn.edu/faculty_scholarship/2035.

Current Progress

In recent years, Internet stakeholders have increasingly promoted routing security, developed initiatives, and provided helpful information (awareness, guidance, training, and monitoring information) to drive down barriers to routing security adoption. Some network service providers have made progress in addressing BGP vulnerabilities; the RPKI framework is now widely accepted as a mature, ready-to-deploy technology and the creation of ROAs, both globally and in North America, has grown steadily. For the first time, the majority of BGP route originations observed on the global Internet are ROV-valid.[31] By some measures, the percentage of Internet traffic volume covered by ROAs has grown to 70.3%.[32]

The North American region is notably different than other regions; it is the oldest and the largest region for Internet address resources. ARIN manages approximately twice the amount of IP version 4 (IPv4) address resources compared to its Asian Pacific or European counterparts.[33] North America has approximately 144,000 ROAs—more than three times as many as the next largest region, Europe, which has approximately 45,000 ROAs.[34]

In the U.S., the percentage of prefixes protected by ROAs is currently 39% ROV-valid.[35] A key problem in the U.S. is select large networks that hold most of the address resources but have lagging ROA rates. For example, the U.S. Federal Government holds approximately 21% of the IPv4 address space in the ARIN region and has had a significantly lower rate of RPKI adoption relative to the private sector.[36] Likewise, there are some very large commercial network providers with complex Internet address inventories and low ROA adoption levels. ARIN data shows commercial network service providers are more likely to have created ROAs than government networks or academic networks[37] and Georgia Institute of Technology data suggests that ROA creation by small networks lags behind large networks.[38] If the low rate of ROA creation and adoption among these few but large network operators that hold a dominant share of North American address space were rectified, BGP security and resilience in the region would substantially improve.

While the state of ROA adoption by ASN can be reasonably measured and monitored from publicly-available data sets, accurately measuring the level of ROV deployment is much more

---

[31] *See* "NIST RPKI Monitor."
[32] Doug Madory and Job Snijders, *RPKI ROV Deployment Reaches Major Milestone*, Kentik Blog, May 1, 2024, https://www.kentik.com/blog/rpki-rov-deployment-reaches-major-milestone/.
[33] *See* "NIST RPKI Monitor."
[34] "Metrics," Routinator, https://rpki-validator.ripe.net/ui/metrics.
[35] *See* "Routing Information in United States," Cloudflare Radar, https://radar.cloudflare.com/routing/us; "State of Routing Security," MANRS Observatory, https://observatory.manrs.org/#/overview.
[36] *Ex Parte Comments of the Internet Society and the Global Cyber Alliance*, In the Matter of Safeguarding and Securing the Open Internet.
[37] *See* John Sweeting, *ARIN Update*, American Registry for Internet Numbers, NANOG 90, February 12, 2024, slides 13-14, https://storage.googleapis.com/site-mediaprod/meetings/NANOG90/4966/20240212_Sweeting_Arin_General_Update_v1.pdf.
[38] *See* Steven Wallace, *The Challenges of RPKI-ROA Diffusion within US R&E*, Internet2, slide 11, https://www.arin.net/vault/participate/meetings/reports/ARIN52/materials/thursday/arin52_keynote.pdf.

difficult.[39] While the various ROV measurement methods and results have differences, there is a general consensus that most Tier 1[40] and many other transit networks providers have deployed RPKI-based technology and are actively filtering ROV-invalid BGP routes from some, if not all, of their neighboring networks.[41] With this level of ROV deployment, RPKI has reached an inflection point; organizations with ROA coverage will reap the benefits, decreasing the likelihood of receiving a false announcement and experiencing a routing incident.[42]

Implementation of ROA and ROV has grown in part due to the concerted efforts and outreach of organizations like the Mutually Agreed Norms for Routing Security (MANRS),[43] as well as the detection and analysis of several significant routing incidents that were, or could have been, avoided with ROV.

Despite these positive trends, there is still work to be done. Today, in the ARIN region, 59% of BGP-announced routes are not covered by ROAs.[44] While in some industry sectors the adoption rate is higher than these averages, in several critical industry sectors the level of adoption is much lower. Even within individual enterprises and service providers, the level of ROA adoption varies across individual ASes. Accelerating RPKI adoption and ROA creation must remain a priority.

Industry and Non-Government Entities

As noted above, there has been significant progress to date by the Internet industry (e.g., IETF, RIRs, hardware/software vendors, and network service providers) to design and establish initial deployments of RPKI, ROA and ROV. Individual stakeholders have also made significant progress in creating, disseminating, and providing information concerning BGP security, including groups and projects like MANRS, the Network Startup Resource Center, Internet2's Routing Integrity Initiative, the North American Network Operators Group conferences, and ARIN training. While these actions are an important catalyst to initial adoption, more effort is needed to expand outreach in specific industry sectors and to complement these stakeholder-led efforts with those of the government.

Federal Government

The U.S. Federal Government is working to implement routing security measures on its networks and is coordinating with private sector stakeholders to amplify the need for collective action.

---

[39] Thomas Hlavacek et al., *Keep Your Friends Close, but Your Routeservers Closer: Insights into RPKI Validation in the Internet*, Proceedings of the 32nd USENIX Conference on Security Symposium, August 9-11, 2023, Anaheim, California, https://www.usenix.org/system/files/usenixsecurity23-hlavacek.pdf.

[40] "Tier 1" service providers are defined in this roadmap as those that are able to reach all Internet endpoints solely through settlement-free peering relationships.

[41] According to researchers at the Georgia Institute of Technology, deployment of ROV in the United States reached 66% of all networks and 89% of Tier 1 (i.e., major ISPs) networks.

[42] *See* Cecilia Testart et al., "To Filter or not to Filter: Measuring the Benefits of Registering in the RPKI Today," Passive and Active Measurement Conference, March 2020, https://catalog.caida.org/paper/2020_filter_not_filter.

[43] Mutually Agreed Norms for Routing Security (MANRS), https://manrs.org/.

[44] *See* "NIST RPKI Monitor."

★ ★ ★ ★ ★ ★

Over the past year, the Office of the National Cyber Director (ONCD) led an effort with ARIN to resolve barriers to Federal agencies' signing of the RSA and develop a Federal RSA template addendum that can be used by Federal departments and agencies to facilitate their adoption of RPKI and other ARIN services.[45] The provisions in this template addendum are supported by Federal laws and principles that necessitated modifications to the requirements in the standard RSA. This addendum was based on pathfinding work by the National Oceanic and Atmospheric Administration (NOAA) and serves as a model for other agencies across the USG.[46]

In May 2024, the Department of Commerce initiated an effort for the creation of ROAs department-wide, signaling the importance for Federal agencies to take a similar approach. NOAA's network service provider, N-Wave, has led in addressing Internet routing security and produced a playbook providing guidance for Federal agencies on ROA implementation.[47]

ONCD strongly encourages Federal departments and agencies to execute a Federal RSA with ARIN as soon as practicable and implement Internet routing security solutions and best practices across the USG. The National Institute of Standards and Technology (NIST) continues to collaborate with USG and industry partners to address remaining BGP security and resilience vulnerabilities by driving the design, standardization, commercialization, and adoption of international standards. NIST's continued efforts to test and measure the completeness and correctness of global RPKI deployments help foster understanding and confidence in emerging BGP security techniques.[48] Additionally, the National Science Foundation (NSF) continues to fund research addressing Internet routing security.

Recommended Actions

Stakeholders within the Internet ecosystem are at different levels of maturity in addressing routing security threats. For each type of network and scope of operation, there are different risk management and cost models associated with adopting new security technologies. Adopting new technologies often follows an incremental deployment approach, where an organization's strategic objectives, cybersecurity plans, and risk management framework should guide the decisions of which networks or routes to secure first.

Organizations should take an informed, *risk-based approach* that identifies, categorizes, and prioritizes the security of the systems, assets, and traffic they consider most valuable and critical to their operations. The following sections outline how to plan and implement ROA and ROV security mechanisms in the context of such an approach. It should be noted that the recommendations that follow are largely consistent with and complementary to those from groups such as MANRS.

---

[45] For USG entities that would like to request a copy of the Federal RSA template addendum, please reach out to FederalROA@ncd.eop.gov.

[46] The Internet2 Routing Integrity program has also reported significant progress in working with ARIN, particularly where academic institutions are state government based, operating under state statutes.

[47] *Federal Resource Public Key Infrastructure (RPKI) Playbook*, NOAA, May 2024, Version 1.3, https://www.noaa.gov/sites/default/files/2024-06/FINAL-Federal-RPKI-Playbook-May-2024.pdf.

[48] *See* "Robust Inter-Domain Routing Project," NIST, https://www.nist.gov/programs-projects/robust-inter-domain-routing.

★ ★ ★ ★ ★ ★

Additionally, in June 2024, as part of ongoing multi-stakeholder efforts to address secure Internet routing concerns, the Federal Communications Commission proposed reporting by network service providers on their progress in implementing measures in BGP plans consistent with the recommended actions for network operators and network service providers outlined below.[49]

Baseline Actions for All Network Operators

The recommended actions below apply to all network types, meaning all network service providers and entities that operate enterprise networks or hold their own IP address resources. These recommendations are of particular importance to the networks used by critical infrastructure,[50] SLTT governments, and any organization dependent on Internet access for purposes that the entity considers to be of high value.

1. **Risk-Based Planning.** Every network operator should develop, maintain, and periodically update a cybersecurity risk management plan. To inform both near- and long-term plans to implement BGP security measures, all network operators should explicitly address the security and resilience of Internet routing in their organization's cybersecurity risk assessment, cybersecurity risk management analysis, and operational plans and procedures. All network operators should consider the following actions in their assessment:
    a. Inventory all Internet number resource holdings, both AS numbers (ASNs) and IP address blocks held by the organization, and identify the various points of contact for each resource.
        i. Identify if any of these address blocks are reassigned from another distinct organization.
        ii. Identify any address blocks that have been reallocated or reassigned to other organizations.
        iii. Identify if each AS and IP address allocation is covered by an RSA with the appropriate RIRs.
        iv. Ensure that up-to-date contact information is entered and maintained in the appropriate RIR databases.
    b. Identify the neighboring ASes with which the organization interconnects to exchange BGP routing information and/or IP data traffic.
        i. For each such network, identify the nature of the business relationship with the other AS (i.e., whether it an upstream transit service provider, a transit services customer, or a peering connection reflecting a settlement-free relationship).

[49] *Reporting on Border Gateway Protocol Risk Mitigation Progress,* PS Docket No. 24-146, Notice of Proposed Rulemaking, FCC 24-62, June 7, 2024, https://docs.fcc.gov/public/attachments/FCC-24-62A1.pdf.
[50] The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters.

c. Document how the organization uses BGP routing by identifying:
    i. Which of the organization's own address prefixes originate from the organization's ASes using BGP announcements;
    ii. Which of the organization's address prefixes rely on the ASes of other organizations to originate their BGP announcements;
    iii. Which address prefixes held by other entities originate from the organization's networks using BGP announcements; and
    iv. Which processes (e.g., inter-domain traffic engineering) or services (e.g., DDoS mitigation services) might alter the origin AS or granularity (i.e., prefix length) of the organization's BGP announcements.
d. Identify information systems and services internal to the organization that require Internet access and the corresponding address prefixes that are announced in BGP to enable that access. Assess the criticality (e.g., organizational mission impact) of maintaining resilient Internet routes for each address prefix originated from the organization's networks or originated on its behalf from other networks.
e. Identify all contracted external/outsourced service providers (e.g., web, DNS, email, storage, etc.) critical to the organization's internal operations and document how routing to and from these services is provided. Assess the criticality of maintaining resilient Internet routes to the organization's external service providers.
f. Establish, communicate, monitor, and maintain a risk management strategy, responsibilities, and policies for Internet routing. This may include evaluating the impact should the availability or integrity of BGP routing to the systems, services, and service providers identified above be disrupted.
g. Based on the organization's cyber risk management strategy, identify address prefixes to prioritize for ROA creation and take action to do so.
    i. Consider prioritizing ROA creation for IP address blocks that contain the most critical services or have the most straightforward routing. In cases where ROA creation is prioritized for different address blocks, identify the specific criteria used for this decision process.
h. Based on the risk management strategy, prioritize ASes for ROV coverage.
i. Continue to monitor developments in BGP routing security, including best practice guidance for adopting new security mechanisms, threat analysis and incident reports, and new developments in standards and their commercialization. Factor any changes in this landscape into future risk management plan revisions.

2. **ROA Publication.** All network operators and entities holding IP address resources should create and publish ROAs in the public RPKI repository hosted by, or delegated from, the appropriate RIR. Operators should use their risk-based cybersecurity risk management plan to prioritize the publication of ROAs for address prefixes they assess as high-value or high-risk first.

3. **Contracting Requirements.** Network operators using contracted external services (e.g., IP transit services, infrastructure services, cloud and content services, etc.) should include explicit requirements in future service contracts for their providers to validate BGP-enabled routes.
4. **Monitoring.** Network operators should monitor the status of their ROA data, routing security threats, outages, and disruptions and assess the quality of their Internet routing services. Such monitoring can be done in-house or contracted through commercial monitoring services.

Additional Actions for Network Service Providers

In addition to the baseline recommendations above, network service providers are uniquely positioned to enhance routing security for the broader ecosystem. These actions include:

1. **ROV Deployment.** Network service providers should deploy ROV filtering for their customers or arrange for upstream providers to do so. Large and small providers alike bear responsibility for ROV filtering, and larger providers are encouraged to implement ROV on behalf of smaller client networks. For organizations with multiple ASNs, consider prioritizing ROV for ASes that propagate the largest number of prefixes and have the largest number of downstream ASes.
2. **Facilitate Customer ROA Creation.** Network service providers that allocate address space to customers should provide tools and guidance to enable their clients to create ROAs—for example, through the network service provider's service portals. Network service providers should provide guidance to their customers encouraging their enrollment in RIR RPKI services. Network service providers should consider providing or creating services to support customers willing to delegate ROA creation to their service providers.
3. **Routing Security Practices Disclosure.** Network service providers should disclose their actions to implement routing security on their networks. Providers should establish a standardized means and format for disclosure of security practices.

Actions for Federal Government and Communications and Information Technology Sector Stakeholder Collaboration

The Federal Government should work collaboratively with communications and information technology (IT) sector stakeholders to take specific action to improve Internet routing security. CISA, as the sector risk management agency for the communications and IT critical infrastructure sectors, in coordination with ONCD and in collaboration with the Communications and IT Sector Coordinating Councils, will establish a joint working group under the auspices of the Critical Infrastructure Partnership Advisory Council to develop resources and materials to advance ROA and ROV implementation and Internet routing security. This effort should include:

1. **Risk Criteria and Prioritization Framework Development.** The working group should develop criteria and a framework for network operators to assess risk and prioritize IP address resources and critical route originations (such as government use, critical

infrastructure operations, etc.)[51] for the application of routing security efforts, to include ROA and ROV. Additionally, the working group should determine meaningful measures of progress and create a standardized set of templates for network service providers to disclose routing security practices.

2. **Network Service Provider Playbook for Customers.** The working group should develop a playbook, informed by diverse industry perspectives and parts of the Internet service ecosystem, that outlines steps for customers to establish ROAs.
3. **Additional Activities and Progress Updates.** The working group should stay informed of updates within the community and deliver a periodic update to the Federal Government that addresses priority issue areas, including:
    a. Whether and how to incorporate additional emerging BGP security standards or mechanisms (as they become commercially available);
    b. Research and development priorities and opportunities;
    c. International engagement efforts to accelerate increased BGP security across the global ecosystem (e.g., harmonizing international standards, reciprocity agreements, and improved partnerships); and
    d. Other areas of interest as determined by the working group.

Policy Actions Specific to the Federal Government

U.S. Federal departments and agencies should implement routing security on their networks, incorporate routing security in procurement requirements, engage in outreach with critical stakeholder communities, assess data from outages caused by routing incidents, promote and incentivize routing security best practices, provide training, reduce barriers to routing security, and monitor threats to routing security.

1. **Guidance to the Federal Enterprise.** The Office of Management and Budget (OMB) should establish guidance for Federal departments and agencies to implement ROAs in a timely manner, aligned with agency risk assessments.
2. **Contracting Requirements.** OMB, working through the Federal Acquisition Regulatory Council and in coordination with the General Services Administration, should require the Federal Government's contracted service providers to adopt and deploy current commercially-viable Internet routing security technologies and perform ROV filtering on the contracted services connecting to the Internet. Federal customers should consult their current network service provider vendors about implementing routing security.
3. **Federal Grant Guidance.** Federal agencies providing grant funding to build critical infrastructure that includes Internet-connected systems or technologies, especially broadband networks, should require grant recipients to incorporate routing security measures into their projects.

[51] Note that IP address assignments may change based on customers, services offered, or the need to perform traffic engineering in response to cyber attacks or changes in traffic load.

4. **Metrics and Progress Reporting.** OMB should establish a reporting mechanism for measuring Federal agency adoption of ROA, monitoring progress, and conducting analytics, where appropriate. The effort should leverage existing data sources and tools provided by academic and third-party partners.
5. **Standards and Technology Development.** NIST should continue to lead and coordinate USG efforts to research, standardize, and foster commercialization of BGP security and resilience mechanisms to address remaining BGP vulnerabilities, including malicious BGP path manipulations, route leak mitigation, and peering authentication. NIST should also continue to develop monitoring and measurement tools to assess the progress and correctness of the global deployment of these additional mechanisms.
6. **Outreach and Education.** CISA, through its public-private engagement efforts, should conduct an outreach campaign to increase U.S.-based enterprise network owners' awareness of the benefits of ROA and ROV. CISA should continue to enhance network defenders' tactical understanding of normal routing behavior, routing anomalies, and route-specific risks that impact network security policy.
7. **International Engagement.** The Department of State, in coordination with appropriate agencies, should highlight Internet routing security efforts and best practices in engagements with international partners to increase awareness of the benefits of the adoption of Internet routing security measures (e.g., RPKI, ROA, and ROV).
8. **Research and Development.** Research-funding agencies (e.g., NSF) should continue to fund the development of Internet routing-focused measurement, monitoring, and alerting technology to facilitate U.S. and global Internet routing security deployment efforts. Funding should support government entities, academic institutions, and independent subject matter experts equipped to measure progress, develop solutions, and inform future innovation. Continued investment should also address the next generation of threats and solutions. The technologies described in this document are appropriate for today, but new threats will evolve, and research is needed to mitigate threats of the future.

Acknowledgements

This *Roadmap to Enhancing Internet Routing Security* is an outcome of the vast amount of time, energy, and expertise dedicated by industry stakeholders and Federal Government representatives reflected in Initiative 4.1.5 of the National Cybersecurity Strategy Implementation Plan.[52] We offer our sincerest gratitude to the technical and policy experts at the National Institute of Standards and Technology, the National Telecommunications and Information Administration, and the Federal Communications Commission for their contributions and guidance. Additionally, we thank the Cybersecurity and Infrastructure Security Agency, the Department of Justice, and the Office of the Director of National Intelligence for their participation and inputs.

We are grateful for the expertise, insight, contributions, and inputs by stakeholder experts from the communications and IT sectors, academia, and the Internet security community in developing this roadmap. Comments on this document may be directed to: FederalROA@ncd.eop.gov.

[52] *The National Cybersecurity Strategy Implementation Plan*, 38.

★ ★ ★ ★ ★ ★

Appendix A: Emerging BGP Security Technologies

Adopting ROAs and ROV addresses one of the fundamental BGP vulnerabilities identified in the introduction of this roadmap. However, continued threats to the security and resilience of the Internet will remain, stemming from BGP's lack of integrity and authentication mechanisms, allowing accidental misconfigurations or malicious actors to manipulate BGP's PATH attributes and spoof the identity of other ASes. The most common example of such manipulations is adding a false origin AS that matches a published ROA to an attempted prefix hijack. These forged origin attacks can undermine the protections provided by ROAs and ROV. Other unauthorized path manipulations can be made to artificially shorten routes, drop ASes from the path that would have resulted in route filtering, or add ASes that would positively influence route selection.

Route leaks are another class of issues that often cause significant failures in Internet routing systems. They are commonly caused by accidental misconfigurations that result in a customer AS forwarding routes learned from one transit provider to another. Such routes violate the business arrangements between ISPs and their clients, and often result in the congestion collapse of smaller networks.

The IETF, RIR communities, and others are working to address these remaining issues. Technologies under development include BGPsec, Autonomous System Provider Authorization (ASPA), Signed Prefix List (SPL) and source address validation using BGP UPDATEs, ASPA, and ROA (BAR-SAV).

- **BGPsec** is an extension to BGP that provides hop-by-hop digital signatures in the BGP PATH element that permits BGPsec-enabled routers to verify the authenticity of each network a route has been propagated through and the integrity of that PATH, ensuring no ASes have been removed from the PATH. BGPsec's PATH signatures rely on the provisioning of keying material in the RPKI. While BGPsec standards were completed in 2017,[53] and prototype reference implementations exist, the standard has yet to be implemented by commercial router vendors. Two barriers exist: 1) BGPsec changes the format of BGP messages, and 2) typical BGPsec implementation requires cryptographic processing of signatures on the routers.
- **ASPA** is an extension to RPKI and BGP that enables ASes to create digitally-signed objects in the RPKI that list the complete set of their upstream transit providers. Designed as a route leak detection and mitigation mechanism, ASPA also provides a form of feasible path verification. ASPA standards are nearing completion in the IETF. Some RIRs already support the creation of ASPA objects in their RPKI, and software router implementations exist.[54]

[53] *See* Matt Lepinski and Kotikalapudi Sriram, *RFC 8205: BGPsec Protocol Specification*, Internet Engineering Task Force, September 2017, https://datatracker.ietf.org/doc/html/rfc8205.
[54] Alexander Azimov et al., "Active Internet Draft: BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects," *Internet Engineering Task Force*, https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification.

- **SPL** is an extension to RPKI that enables an AS to publish a digitally-signed list of all the prefixes it originates. This is similar to a ROA, except it is signed by the AS holder, rather than the prefix holder. SPL extends ROV with a second data source that mitigates AS forgery and reduces the attack surface for forged origin attacks.[55]
- **BAR-SAV** is a mechanism that uses BGP updates and ROA and ASPA data to build more accurate source address validation (anti-spoofing) filters.[56] BAR-SAV is a DDoS mitigation mechanism that leverages emerging BGP security technologies to construct better filters.

Each of these specifications are at different stages of maturity within the IETF, and the commercial viability of these techniques has yet to be established. More research, development, testing, and guidance is needed before they are incorporated into future adoption plans, such as those outlined in this roadmap. They are included here for awareness and further discussion.

[55] Kotikalapudi Sriram, Job Snijders, and Doug Montgomery, *Active Internet Draft: Signed Prefix List (SPL) Based Route Origin Verification and Operational Considerations*, Internet Engineering Task Force, June 14, 2024, https://datatracker.ietf.org/doc/draft-ietf-sidrops-spl-verification.

[56] *See* Kotikalapudi Sriram, Igor Lubashev, and Doug Montgomery, *Active Internet Draft: Source Address Validation Using BGP UPDATEs, ASPA, and ROA (BAR-SAV)*, Internet Engineering Task Force, March 4, 2024, https://datatracker.ietf.org/doc/draft-ietf-sidrops-bar-sav/.