COMMENTS OF INTERNET SOCIETY

Introduction

The Internet Society (ISOC)[1] appreciates the opportunity to make a submission on the Australian Cyber Security Strategy (the 'Strategy') Discussion Paper. Our submission focuses on questions pertinent to our areas of expertise, and to Internet security in particular.

Today, the Internet plays an essential role in economies around the world. From banking to education, health to logistics, just about every sector relies on Internet-based applications and services to function.

Our increased dependence on digital technologies brings with it growing concerns around Internet security, a subset of Cybersecurity involving the global Internet and associated network resources. While there are many dimensions to Cybersecurity, securing the key building blocks of the Internet's infrastructure is critical.

The Internet consists of multiple layers, each with its unique function along with vulnerabilities and risks. Therefore, it is crucial to ensure that cybersecurity covers every layer of the Internet whether it is physical cables, networks and routing or the application layer to ensure the safety and security of the digital ecosystem.

Specific Responses to Questions

We have specific responses to several questions from the Strategy Discussion Paper.

[1] Founded by Internet pioneers, the Internet Society is a non-profit organization dedicated to ensuring the open development, evolution, and use of the Internet. Working through a global community of chapters and members, the Internet Society collaborates with a broad range of groups to promote the technologies that keep the Internet safe and secure, and advocates for policies that enable universal access. The Internet Society is also the organizational home of the Internet Engineering Task Force (IETF).

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

The Internet Society would like to emphasize the importance of including network and routing security as part of the overall Cybersecurity strategy.

Network and routing security are critical components of cybersecurity. A secure network is essential to protect against cyber threats, and to ensure the confidentiality and integrity of information, and the resiliency of associated infrastructure.

Routing security plays a pivotal role in ensuring the overall security of a network. Routing refers to the process of directing data packets from one network to another, and routing protocols are the rules that govern this process. Border Gateway Protocol (BGP) is the routing protocol of the Internet that allows different networks to talk to each other and efficiently route traffic across the Internet.

BGP (Border Gateway Protocol) provides a set of rules that network operators (whether they are Internet service providers (ISPs) or enterprises connecting to the Internet) use to talk to each other and exchange information about the best way to route traffic between their networks. Without BGP, the Internet would not be able to function because all the different networks would not know how to communicate with each other.

While BGP is a critical component of the Internet's infrastructure, it is also vulnerable to various security risks and vulnerabilities. These can be exploited by attackers to disrupt network traffic or redirect it to malicious destinations. As a result, routing security has become a critical concern in cybersecurity. Without proper routing security measures in place, an organization's network could be vulnerable to a wide range of attacks such as route hijacks[2] and route leaks. Implementing routing security is an essential part of a healthy cybersecurity regime.

The United States' National Cybersecurity Strategy 2023[3] also highlights the issues with BGP "*We must take steps to mitigate the most urgent of these pervasive concerns such as Border Gateway Protocol vulnerabilities, unencrypted Domain Name System requests, and the slow adoption of IPv6*".

[2] Meynell, Kevin. 2020. "What are Routing Incidents? (Part 4)". MANRS. https://manrs.org/2020/07/what-are-routing-incidents/ .
[3] United States of America. Mar. 2023. "National Cybersecurity Strategy". White House. https://whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf .

In recent years, adoption of routing security best practices has accelerated significantly across the globe thanks to community/Industry efforts such as Mutually Agreed Norms for Routing Security (MANRS).

MANRS[4] is a global community driven initiative, supported by the Internet Society, that provides a set of best practices based on existing norms which provides crucial fixes to reduce the most common Internet routing threats. MANRS offers specific actions via tailored programs[5] for Network Operators, Internet Exchange Points, CDN and Cloud Providers, and Equipment Vendors.

We are pleased to see that MANRS is highlighted in the Australian Signals Directorate (ASD)'s gateway security guidance package[6] published in July 2022 where government organizations are encouraged to include MANRS actions compliance in making procurement decisions.

We strongly suggest that this recommendation be extended to every organization in Australia connected to the Internet. The Cybersecurity Strategy's endorsement of routing security norms provided by MANRS will help protect the overall Internet routing infrastructure in the country, elevate its cybersecurity posture and work to ensure that Australia plays its role in supporting an open, globally-connected, secure and trustworthy Internet.

[4] https://www.manrs.org/

[5] https://www.manrs.org/programs

[6] Australian Signals Directorate. 2022. "Gateway Security Guidance Package: Gateway Operations and Management". Australian Cyber Security Centre. https://cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/gateway-secuirty-guidance/gateway-operations-management .

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

The Internet ecosystem is rapidly evolving, with new technologies, standards, protocols, platforms, and services constantly emerging. As such, it can be challenging to develop and enforce laws and regulations that keep up with the changing nature of the Internet. While there are proactive actions the Australian Federal Government can take to improve routing security as we suggest in response to Question 1, we caution against prescriptive routing security mandates across the board which could have serious unintended consequences because we firmly believe that the Internet industry is better governed by norms rather than laws.

Norms are more flexible and adaptable as compared to laws, which can be rigid and slow to change. As the Internet industry evolves, norms can adapt to new technologies and practices more quickly. They are often developed collaboratively by stakeholders in the Internet industry, including expert tech groups, civil society organizations, and governments. This collaborative approach[7] can promote shared values and goals, leading to greater cooperation and trust among stakeholders. It also encourages innovation by promoting best practices, encouraging experimentation, and fostering a culture of continuous improvement.

Norms developed collaboratively by industry groups and civil society organizations such as MANRS can play an effective role on their own, but government engagement and support are essential to develop a relevant and comprehensive cybersecurity strategy for the country—and even for the region.

The Australian Federal Government can leverage their understanding of the regulatory frameworks in the region by promoting international cooperation, providing cybersecurity expertise and resources, and ensuring accountability. It can play a vital role in protecting the public interest and ensuring the security of critical infrastructure and sensitive data.

Given the increasing momentum among network operators to implement routing security best practices, we recommend that the Advisory Board review the new report from the Organization for Economic Co-operation and Development (OECD), *Routing security: BGP incidents, mitigation techniques*

[7] Internet Society. "Collaborative Security". https://internetsociety.org/collaborativesecurity/ .

and policy actions.[8] The OECD's report provides an overview of the vulnerabilities in the routing system, approaches to manage the risks associated with those vulnerabilities, and incentives to deploy necessary security controls. The OECD's report also includes four policy recommendations, focused on accelerating improvements in routing security:

1. *Promote measurement:* the report observes a lack of longitudinal studies and high-quality data sources for routing information and routing security data, which can prevent or delay informed decision making.
2. *Promote awareness:* the report identifies a role for policy makers in raising awareness around routing security, with examples such as the Dutch 'comply or explain' procurement process.
3. *Facilitate information sharing:* the report calls for clear mechanisms to share information on routing incidents between stakeholders. Interestingly, the report mentions the realm of Computer Emergency Response Teams (CERTs) but does not mention the role of information sharing in network operator groups.
4. *Define a common framework with industry to improve routing security:* the report calls for governments to work with industry and technical experts on a framework that would establish targeted actions to improve routing security within a set time frame. It calls for a multistakeholder approach, using MANRS as an example. But this section also talks about the threat of regulation that could put the technical community in motion.

[8] Organization for Economic Development (OECD). Oct. 2022. "Routing security: BGP incidents, mitigation techniques and policy actions". OECD Publishing. https://oecd.org/publications/routing-security-40be69c8-en.htm.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

The Australian Federal Government, and its various agencies, can use its influential role as a corporate customer to incentivize better routing security practices by strengthening procurement requirements. These are already highlighted in the Australian Signals Directorate (ASD)'s gateway security guidance package published in July 2022, and includes routing security best practices for network services. The Federal Government can help encourage industry to implement these best practices.

Implementation of important best practices like Resource Public Key Infrastructure ("RPKI")[9], which is a security framework network operators can use to validate and secure the critical route updates or Border Gateway Protocol (BGP) announcements between public Internet networks, has improved substantially among network operators globally. Since March 2021, the global percentage of valid routes using RPKI has almost doubled, from 28% to 42% as of March 2023. There are concerns around the efficacy of RPKI given its lack of wider deployment but at the current rate of deployment of route origin validation (ROV), RPKI-invalid routes have already reduced propagation of bad routes "by *anywhere between one half to two thirds.*"[10]

Despite the recent progress in routing security, including RPKI deployment, there are still challenges that need to be addressed. In Australia there are more than 1500 network operators and cumulatively they all lag behind the global average for RPKI deployment. As of March 2023, only 34.2% of their routes have valid Route Origin Authorizations (ROAs). With the current rate of RPKI ROA adoption, Australia will continue to be falling behind considerably.

[9] RPKI [ROV and ROA] - The most widely known application of RPKI is Route Origin Validation (ROV). ROV is a route-filtering process that is executed using Route Origin Authorizations (ROAs), which are cryptographically signed objects that state which Autonomous System (AS) is authorized to originate a particular IP address prefix or set of prefixes. ROV software then verifies the data from trust anchors. Once validated, ROAs can be used to generate route filters. This process, using ROAs to perform ROV to classify routes as invalid or not, allows networks on the Internet to ignore bad route announcements that are invalid and may be erroneous or malicious in nature.

[10] Madory, Doug; Snijders, Job. 2022. "How much does RPKI ROV reduce the propagation of invalid routes?". Kentik Blog. https://kentik.com/blog/how-much-does-rpki-rov-reduce-the-propagation-of-invalid-routes/ .

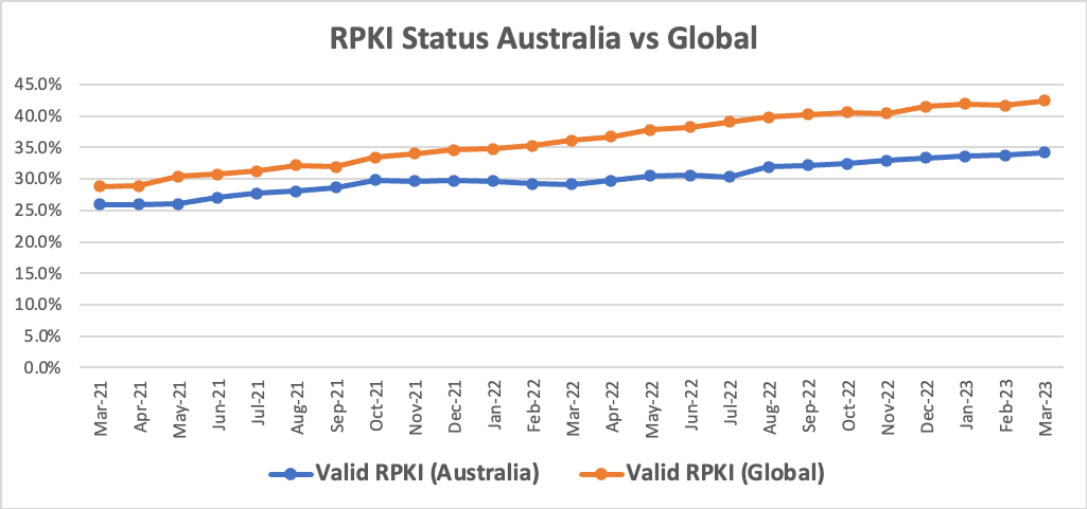

Figure1: Percentage of Route Announcements with RPKI validated prefixes from Australian networks vs Global networks between March 2021 to March 2023. Data collected from the MANRS Observatory[11]

The Federal Government has an opportunity to lead by example in Internet routing security by implementing best practices on their own networks. It can also encourage State and Territory Governments to do the same as well.

[11] https://observatory.manrs.org/#/history

10. What best practice models are available for automated threat-blocking at scale?

In the Internet network and routing security area, the following best practice models are very well accepted by industry.

MANRS:

MANRS defines four simple but concrete actions for network operators to implement and greatly improve Internet security and reliability. All these actions are technology agnostic and have proven to provide protection from various types of routing attacks.

1. **Filtering** – defining a clear routing policy and implementing a system to ensure that announcements to adjacent networks are correct.
2. **Anti-spoofing** – enabling source address validation (SAV) and implementing anti-spoofing to prevent packets with incorrect source IP addresses from entering and leaving the network.
3. **Coordination** – maintaining globally accessible up-to-date contact information to assist with incident response.
4. **Global validation** – publishing data that enables other stakeholders to validate routing information on a global scale.

More than 915 networks across the world are part of the MANRS initiative and have committed to implementing the basic routing security hygiene to protect not only their own networks but their customers as well. MANRS initiative participants have helped increase the overall RPKI adoption rate in Australia as well. For example, MANRS participants in Australia have a 61% RPKI adoption rate whereas non-MANRS participants are at 34.2%.

Major MANRS participants in Australia include Telstra, Vocus, Aussie Broadband, Superloop, Real World Technology Solutions, AARNET, and EDGE-IX.

NIST SP1800-14:

The US-based National Institute of Standards and Technology (NIST) publishes Cybersecurity Practice Guides (Special Publication Series 1800) which targets specific cybersecurity challenges in the public and private sectors. These are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity.

They show members from the information security community how to implement example solutions that help them align more easily with relevant standards and best practices. They provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

NIST has published Special Publication 1800-14, *Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation*[12]. This Cybersecurity Best Practice Guide demonstrates how networks can protect BGP routes from vulnerability to route hijacks by using available security protocols, products, and tools to perform BGP Route Origin Validation (ROV) and reduce route hijacking threats.

[12] Computer Security Resource Center. Jun. 2019. "Protecting Integrity of Internet Routing BGP Route Origin Validation". U.S. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/1800-14/final .

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

Cybersecurity has many layers and dimensions and can be best addressed via multistakeholder collaboration. Government should work with all stakeholders including industry, academia, and research institutes to share information, improve cybersecurity best practices and build a knowledgebase which can eventually change behaviors through education and awareness.

Government should invest in cyber security education and training programs for their own employees and partners. This can include offering courses, seminars, and certifications on cybersecurity best practices and technologies provided by industry experts. Organizations such as the Internet Society with its Learning @ Internet Society resource[13], the NSRC (Network Startup Resource Centre) World YouTube Channel[14] and the APNIC Academy[15] provide many online and in-person training opportunities that address these issues.

While the Internet industry is better served by norms, Government can establish certain standards for cybersecurity practices in the financial, healthcare, and critical infrastructure sectors. These standards can help organizations prioritize their cybersecurity efforts and ensure that they are meeting minimum security requirement – both for them and their customers and users.

Government could also offer incentives to organizations that demonstrate strong cybersecurity practices, such as tax credits or preferential treatment in government contracts. This can encourage organizations to prioritize cybersecurity and invest in the necessary resources to protect their systems, data, and users.

On-going support for research and development in the cybersecurity arena is very critical. Government can act as a facilitator and collaborate with industry and the research community on projects aimed at improving cybersecurity technologies and best practices. This can help in the development of new solutions to combatting emerging threats and vulnerabilities and help build a cybersecurity industry for domestic and international markets.

[13] https://www.internetsociety.org/learning
[14] https://www.youtube.com/user/NSRCworld
[15] https://academy.apnic.net/en

Conclusion

Thank you for the opportunity to submit comments and provide some answers to questions in the Strategy Discussion Paper. We look forward to responding to any additional questions that may arise in the proceeding.

Respectfully submitted,
By:

Rajnesh Singh
Regional Vice President - Asia-Pacific

Joseph Lorenzo Hall
Distinguished Technologist, Strong Internet

Aftab Siddiqui
Senior Manager, Internet Technology, Asia-Pacific

Kevin Meynell
Senior Manager, Technical and Operational Engagement

Internet Society
11710 Plaza America Drive
Suite 400
Reston, VA 20190
703-439-2120