21 May 2019

MANRS Implementation Guides RIPE BCOP Task Force



Kevin Meynell Manager, Technical & Operational Engagement meynell@isoc.org

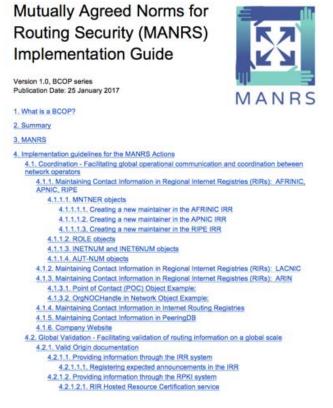
Internet Society © 1992–2017

What is the MANRS Initiative?

- Mutually Assured Norms for Routing Security (MANRS) promotes routing security best practices
- Aims to mitigate route leaks, route hijacks and spoofing that have been a growing problem on Internet
- MANRS defines four simple but concrete actions to improve Internet security and reliability:
 - Filtering Prevent propagation of incorrect routing information (CIDR Report & BGPStream)
 - Anti-spoofing Prevent traffic with spoofed source IP addresses (CAIDA Spoofer)
 - Coordination Facilitate global operational communication (Whois & PeeringDB)
 - Global Validation Facilitate validation of routing information on a global scale (IRR & RPKI)
- MANRS is based on existing tools and techniques, and established industry best practices (RIPE community has been an important source of input and review)
- Two significant categories of MANRS participants: Network Operators and IXPs
- See https://www.manrs.org for more information

MANRS Implementation Guide for Network Operators

- The MANRS Implementation Guide for Network Operators was published in January 2017
 - Provides technical and configuration information on how to deploy each of the MANRS Actions
 - Authored by David Freedman, Brian Foust, Barry Greene, Ben Maddison, Andrei Robachevsky, Job Snijders, Sander Steffann, Will van Gulik, Jakob Heitz, Aris Lambrianidis, Kevin Meynell and Massimiliano Stucchi
 - Abridged version was published as ripe-706
- Looking for volunteers to review and possibly update this document



MANRS Implementation Guide for IXPs

- Looking to develop similar Implementation Guide for MANRS IXP Actions
- MANRS IXP Actions:
 - Action 1: Use route server to validate route announcements from peers (using IRR and/or RPKI)
 - Action 2: Encouraging IXP members to employ MANRS (via capacity building, discounting, acclaim)
 - Action 3: Layer 2 filtering
 - Action 4: Ensure every member is contactable and responsive in mitigating network incidents
 - Action 5: Provide monitoring and debugging tools for routing incidents/anomalies (e.g. Looking Glass)
- Something similar needed for IXPs on how to implement these Actions?
- ISOC can provide editor (me), but any subject matter experts willing to contribute content towards this?
- Can also be submitted as RIPE Document

Thank you.

Kevin Meynell meynell@isoc.org Visit us at www.internetsociety.org Follow us @internetsociety Galerie Jean-Malbuisson 15, CH-1204 Geneva, Switzerland. +41 22 807 1444 1775 Wiehle Avenue, Suite 201, Reston, VA 20190-5108 USA. +1 703 439 2120