CableLabs

Driving More Secure Internet Routing

Introducing a “Cybersecurity Framework Profile for Internet Routing”

APNIC 57 | APNIC Routing Security SIG | February 29, 2024

Priya Shrinivasan

Director, Technology Policy

p.shrinivasan@cablelabs.com

Summary

- CableLabs, its members, and NCTA – the Internet and Television Association developed a Cybersecurity Framework (CSF) Profile for Internet Routing (Routing Security Profile or RSP).
- The RSP is a compilation of the cable industry's expertise, aligned with the National Institute of Standards and Technology (NIST) CSF v1.1, that provides a roadmap for any organization to drive more secure internet routing.
- The cable industry has long recognized the threats to internet routing and has proactively sought to address those threats both internally and through broader industry technical fora.
- Our next step is to take the RSP to the broader internet community to drive awareness and to further advance this work.

WHO WE ARE

CableLabs is the global broadband industry's leading R&D lab for next-generation network technologies

OUR MEMBERS SPAN THE GLOBE

Our 60-plus members, who include leading cable operators, span more than 35 countries and serve over 150 million households and mobile users.

OUR TECHNOLOGIES

- Advanced Optics & Fiber
- AI & Machine Learning
- Cloud Native
- Convergence
- Hybrid Fiber Coax
- Immersive Media
- Mobile
- Security & Privacy
- Quantum Networks
- Wi-Fi

Over half a billion people use our technologies every day*

*Based on member subscriber numbers

The Road to the Routing Security Profile

Background – Increased Governmental Interest and Focus

- US Federal Communications Commission (FCC) Secure Internet Routing NOI (Feb 2022) and FCC Public Border Gateway Protocol (BGP) Security Workshop (July 31, 2023)

- US National Cybersecurity Strategy (March 2023): "*We must take steps to mitigate the most urgent of these pervasive concerns such as Border Gateway Protocol vulnerabilities…*" and National Cybersecurity Strategy Implementation Plan (July 2023)

- US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Concept Paper (January 2023): *call to action to submit examples of "profiles" mapped to the CSF aimed at addressing cybersecurity risks associated with a particular business activity of operation*

Profile Development Work Group Members:

CableLabs®

ncta
THE INTERNET & TELEVISION ASSOCIATION

ARMSTRONG®

Charter
COMMUNICATIONS

COMCAST

COX®

eastlink

LIBERTY GLOBAL

MIDCO®

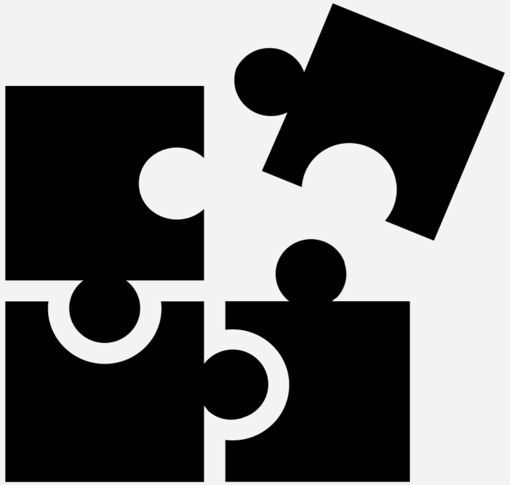
ROGERS™

VIDEOTRON

Cybersecurity Framework Profile for Internet Routing (RSP)

What is the Routing Security Profile (RSP)?

- The RSP is a framework for improving security and managing risks for internet routing, which is *one key piece of a larger critical infrastructure cybersecurity puzzle.*
- It approaches routing security from a holistic, risk management perspective.
- It is applicable for use by any autonomous system (AS) operator – large or small – to enhance routing security.



What is the Routing Security Profile? (Continued)

- The RSP is based on NIST CSF v1.1. [Note: CSF 2.0 was released a few days ago on February 26, 2024]
- The NIST CSF consists of three main components: the Core, Implementation Tiers, and Profiles
    - Core – “provides a set of desired cybersecurity activities and outcomes using common language that is easy to understand”
    - Implementation Tiers – “assist organizations by providing context on how an organization views cybersecurity risk management”
    - Profiles – “primarily used to identify and prioritize opportunities for improving cybersecurity at an organization”

Goals of the Routing Security Profile

- The RSP serves as a foundational tool for network engineers, IT managers, cybersecurity professionals and decision-makers involved in network security risk management to evaluate, implement, and manage robust routing security policies.
- It aims to be adaptable and scalable to not only aid AS operators as they fortify their own network environments but also contribute to the broader goal of creating a more secure and resilient global internet infrastructure.

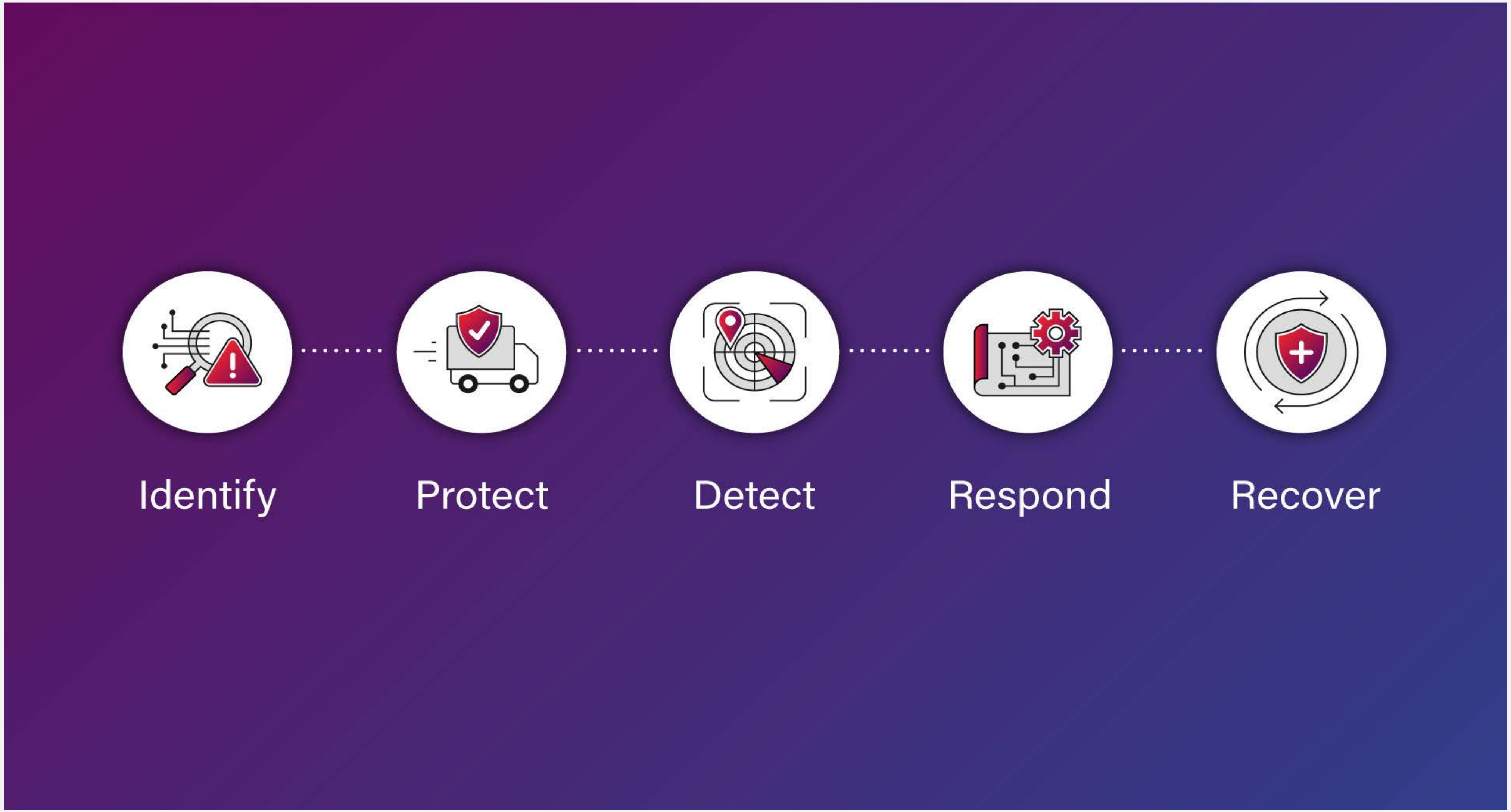
Scope of the Routing Security Profile

- Focuses on routing security within network infrastructures, including a network service provider's routing infrastructure, security infrastructure supporting routing security, external routing peering interfaces, and external routing information registries.
  - Border Gateway Protocol (BGP) security
  - Internet Routing Registries (IRRs)
  - autonomous system (AS) path filtering
  - Resource Public Key Infrastructure (RPKI)
  - ROA (Route Origin Authorization) objects
  - ROV (Route Origin Validation)
  - Operations, Administration, and Management (OAM) systems
- Does not cover general cybersecurity topics unrelated to routing, nor the security aspects of other network layers or services.

Using the Routing Security Profile

- The RSP customizes the CSF v1.1 structure by mapping routing security best practices and informative references to the applicable categories and subcategories of a CSF core function.
- For each core function category, a table lists the subcategories, their applicability to routing security, and related informative references.
- Informative references (e.g., NIST standard, IETF RFC, or RPKI BCP) included in the tables provide additional guidance to aid practitioners when applying the RSP.
- Practitioners are urged to review all subcategories (including those considered not applicable to routing security) in the context of their organization and adapt as needed to accommodate their organization's unique environment and needs.

Cybersecurity Framework Profile for Internet Routing (Based on NIST CSF 1.1)



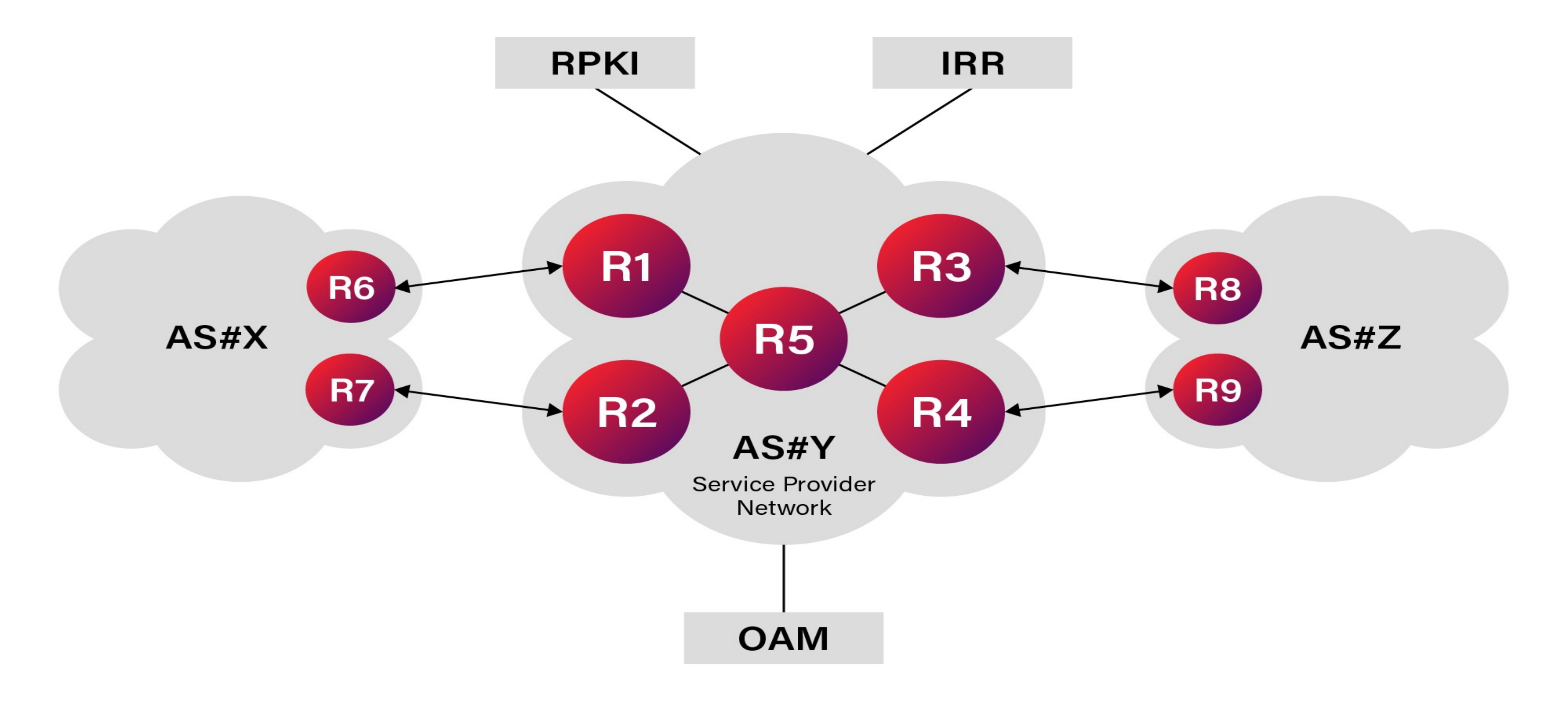
Cybersecurity Framework Profile for Internet Routing – Sample of Identify: Asset Management Category

Subcategory	Applicability to Routing Security	Informative References
ID.AM-1: Physical devices and systems within the organization are inventoried	Routing hardware should be inventoried, including BGP routers and computing devices used for RPKI and management functions.	NIST SP 800-53 Rev. 5: CM-8, PM-5
ID.AM-2: Software platforms and applications within the organization are inventoried	Routing software elements should be inventoried, including BGP router software, operating systems used by all relevant computing devices, the RPKI validator, and cryptographic packages such as used for RPKI Certification Authority.	NIST SP 800-53 Rev. 5: CM-8, PM-5
ID.AM-3: Organizational communication and data flows are mapped	Routing information such as policies, ACLs, routes, etc., should be mapped to understand what information needs to be protected, who has access, and why.	NIST SP 800-53 Rev. 5: AC-4, CA-3, CA-9, PL-8
ID.AM-4: External information systems are catalogued	External routing information such as routes, ROAs, and IRRs are cataloged.	NIST SP 800-53 Rev. 5: AC-20, SA-9

Sample of Identify: Asset Management Category (Continued)

Subcategory	Applicability to Routing Security	Informative References
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Applicable, no routing-specific considerations.	NIST SP 800-53 Rev. 5: CP-2, RA-2, SA-14, SC-6
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	The cybersecurity roles and responsibilities for securing the routing infrastructure and third-party stakeholders (e.g., RIRs, IRRs, peering partners) are established.	NIST SP 800-53 Rev. 5: CP-2, PS-7, PM-11

Identify - Asset Management Subcategory



Key Takeaways

- Threats to internet routing are diverse, persistent, and changing.
- Current efforts focus on developing and implementing security controls (e.g., RPKI).
- The RSP approaches routing security from a holistic, risk management perspective and is applicable for use by any Autonomous System (AS) operator to enhance routing security.
- The RSP is a tool for practitioners and network operators to advance routing security of any size organization – large or small.
- The RSP and the underlying technical controls must remain agile and continue to evolve to stay ahead of a constantly changing threat landscape.

Next Steps

- Engage with broader internet ecosystem stakeholders – like all of you – to drive awareness and to further improve and advance this work for all AS operators, including ISPs, cloud service providers, government agencies, universities, and other organizations.
- Update this first version of the RSP based on feedback received from stakeholders and to reflect changes in the NIST CSF 2.0 (released just a few days ago).

Questions?

https://www.cablelabs.com/blog/
internet-routing-security-framework