CableLabs®
Security

Cybersecurity Framework Profile for Internet Routing

CL-GL-RS-Profile-V02-241001

RELEASED

DISCLAIMER

This document is furnished on an "AS IS" basis and neither CableLabs nor its members provide any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, infringement, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	CL-GL-RS-Profile-V02-241001			
Document Title:	Cybersecurity Framework Profile for Internet Routing			
Revision History:	V01 – Released 01/23/2024 V02 – Released 10/01/2024			
Date:	October 1, 2024			
Status:	~~Work in Progress~~	~~Draft~~	**Released**	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/Member/ Vendor~~	**Public**

Key to Document Status Codes

Work in Progress	An incomplete document designed to guide discussion and generate feedback.
Draft	A document that is considered largely complete but is undergoing review by working groups, members, and vendors. Drafts are susceptible to substantial change during the review process.
Released	A public or gated document that has undergone review. Released guidelines are **not** subject to the Engineering Change process.
Closed	A static document that has been closed to further changes through CableLabs.

Trademarks

Contents

Figures

Tables

Executive Summary

This routing security profile provides informative guidelines to assist network operators, cloud service providers, and other organizations—large and small—in managing routing security risks and implementing best practices that are aligned with the NIST Cybersecurity Framework (CSF) 2.0. Without necessary security controls, routing infrastructure and protocols like the Border Gateway Protocol (BGP) are vulnerable to attack and misconfiguration, which can lead to network disruptions including data leakage, network outages, and unauthorized access to sensitive information. Global communications rely on an internet that is reliable and secure.

This routing security profile covers not only hardware, software, and service infrastructure, but also core routing protocols, including BGP, and emerging technologies like resource public key infrastructure (RPKI). It serves as an adaptable and actionable guide for network engineers, security analysts, and executives to evaluate and enhance routing security, stability, and resilience. This routing security profile contains a catalog of considerations related to improving routing security, including route origin authorization (ROA), route origin validation (ROV), BGP peer authentication, prefix filtering, and monitoring for routing anomalies. Adopting this profile will enable organizations to proactively identify and mitigate routing threats, facilitate communication on priorities, and ultimately build resilient foundations capable of withstanding emerging threats to the security of internet routing.

1 SCOPE

1.1 Introduction and Background

The modern world is heavily reliant on networked systems for communications, financial transactions, healthcare services, and various other critical aspects of daily life. With the increasing complexity and ubiquity of network infrastructures, the security of routing protocols and routing devices becomes an integral facet of the cybersecurity landscape. Malicious actors and threat vectors targeting the routing layer can lead to severe disruptions, including data leakage, network outages, and unauthorized access to sensitive information.

Routing security has been an oft-underappreciated aspect of a secure network, overshadowed by more visible security elements like firewalls or intrusion detection systems. However, the integrity of routing processes is essential for ensuring that data packets safely reach their intended destinations without being intercepted, altered, or dropped. Inadequate routing security can make the entire network susceptible to attacks, such as Internet Protocol (IP) spoofing, route hijacking, and man-in-the-middle attacks.

This routing security profile, based on the NIST Cybersecurity Framework 2.0, has three goals.

1. Provide a comprehensive set of guidelines, best practices, and strategies to secure the routing infrastructure within an organization—The profile is intended to serve as an actionable and adaptable guide to managing risks and improving the security posture of routing environments. The framework aligns routing security best practices with industry standards to enable organizations to evaluate, implement, and manage robust routing policies.
2. Focus on IP networks using BGP, addressing its inherent vulnerabilities and proposing countermeasures—The profile serves as a foundational tool for network security engineers, administrators, and decision-makers to evaluate, implement, and manage robust routing security policies.
3. Mitigate risks and ensure the confidentiality, integrity, and availability of data as they traverse complex network pathways—The profile also aims to be adaptable and scalable, capable of evolving along with emerging technologies and threats.

By adopting this routing security profile, organizations not only fortify their own network environments but also contribute to the broader goal of creating a more secure and resilient global internet infrastructure.

1.2 Purpose and Objectives

This routing security profile provides informative practical guidance for organizations and stakeholders engaged in the design and operation of IP networks in a manner consistent with the organization's risk tolerance. It is suitable for applications that involve multiple stakeholders contributing to IP network operation and architectures. Use of the routing security profile will help organizations

- govern cybersecurity risks, including supply chain risks, to IP networks;
- identify systems, assets, data, and risks that pertain to IP networks;
- protect IP networks by performing self-assessments and adhering to cybersecurity principles;
- detect cybersecurity-related disturbances or corruption of IP network services and data;
- respond to IP network service or data anomalies in a timely, effective, and resilient manner; and
- recover the IP network to proper working order after a cybersecurity incident.

1.3 Scope

This document focuses exclusively on routing security within network infrastructures (Figure 1), including a network service provider's routing infrastructure, security infrastructure (such as RPKI) supporting routing security, external routing peering interfaces, and external routing information registries (e.g., IRRs). It aims to provide a

comprehensive framework for managing, implementing, and monitoring security measures related to routing protocols and services. The scope encompasses but is not limited to the following.

- 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

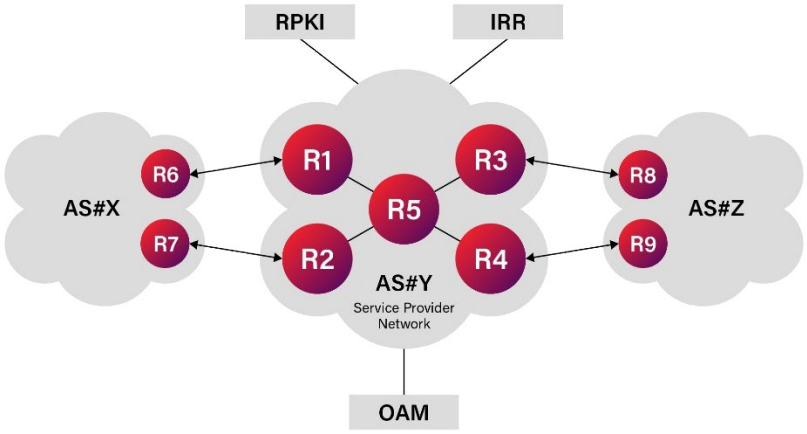

Figure 1 - Service Provider Network Routing Infrastructure

The routing security profile is designed to be applicable to a variety of organizations, including internet service providers (ISPs), enterprise networks, and cloud service providers. It is intended for use by network engineers, IT managers, cybersecurity professionals, and decision-makers involved in network security risk management.

This document does not cover general cybersecurity topics unrelated to routing, nor does it delve into the security aspects of other network layers or services. It is meant to augment, not replace, existing security policies and risk management procedures within an organization.

1.4 Audience

This document is intended for those involved in managing, developing, implementing, and monitoring routing security in network infrastructures:

- network engineers responsible for the configuration and maintenance of routing protocols like BGP;
- ISPs that need to implement routing security measures such as RPKI, IRRs, and AS path filtering;
- IT managers overseeing network operations and routing policies;
- risk managers, cybersecurity professionals, and others involved in network security risk management;
- business and mission-critical process owners who rely on secure and stable routing for operational outcomes;
- researchers and analysts focused on the cybersecurity aspects of network routing; and
- network architects who integrate routing security measures into network designs.

1.5 Intended Use

This routing security profile is intended to be used as part of an overall risk management strategy for networks, with a focus on routing security. It is intended to provide actionable, practical guidance for organizations to assess their current security posture and inform future decisions related to routing protocols like BGP, RPKI, IRRs, and AS path filtering. It also can be used as part of a larger, in-depth security assessment.

Below are some considerations to aid organizations as they assess and customize this profile for their unique needs.[1]

- Mission Considerations
  - What routing services are mission critical?
  - What network elements and data/assets are vulnerable to routing attacks?
  - What recovery/fail-over strategies can be employed for routing?
  - What metrics are available to determine the effectiveness of routing security controls?
- Engineering Considerations
  - What are the routing capabilities of the network?
  - What are the capabilities of potential adversaries targeting routing?
  - Which routing attributes can be adjusted post-deployment, and which are immutable?
- Operational Considerations
  - What methods can be used to detect potential routing anomalies?
  - What methods can be used to respond to detected routing issues?
  - What methods can be employed for post-event routing recovery?
- External Considerations
  - What external routing services and data are critical?
  - What are the impacts of degraded or failed external routing services?

[1] This Routing Security Profile was modeled after and developed using the overall structure of the NIST Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN). [NIST IR 8441].

2 REFERENCES

2.1 Informative References

This guideline uses the following informative references. These informative references provide additional guidance to aid practitioners when applying this profile.

[NIST CSF 1.1] NIST Cybersecurity Framework v1.1, April 2018, https://www.nist.gov/cyberframework/framework

[NIST CSF 2.0] NIST Cybersecurity Framework v2.0, February 2024, https://www.nist.gov/cyberframework/framework

[NIST IR 8441] NIST IR 8441, Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN) [initial public draft], J. McCarthy and others, June 2023, https://doi.org/10.6028/NIST.IR.8441.ipd

[NIST SP 800-189] NIST SP 800-189, Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation, K. Sriram, D. Montgomery, December 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189.pdf

[RFC 2385] IETF RFC 2385, "Protection of BGP Sessions via the TCP MD5 Signature Option," A. Heffernan, August 1998

[RFC 4253] IETF RFC 4253, "The Secure Shell (SSH) Transport Layer Protocol," T. Ylonen, C. Lonvick, January 2006

[RFC 4272] IETF RFC 4272, "BGP Security Vulnerabilities Analysis," S. Murphy, January 2006

[RFC 5082] IETF RFC 5082, "The Generalized TTL Security Mechanism (GTSM)," V. Gill, J. Heasley, D. Meyer, P. Savola, October 2007

[RFC 5925] IETF RFC 5925, "The TCP Authentication Option," J. Touch, A. Mankin, R. Bonica, June 2010

[RFC 6480] IETF RFC 6480, "An Infrastructure to Support Secure Internet Routing," M. Lepinski, S. Kent, February 2012

[RFC 6482] IETF RFC 6482, "A Profile for Route Origin Authorizations (ROAs)," M. Lepinski, S. Kent, D. Kong, February 2012

[RFC 6488] IETF RFC 6488, "Signed Object Template for the Resource Public Key Infrastructure (RPKI)," M. Lepinski, A. Chi, S. Kent, February 2012

[RFC 6810] IETF RFC 6810, "The Resource Public Key Infrastructure (RPKI) to Router Protocol," R. Bush, R. Austein, January 2013

[RFC 6811] IETF RFC 6811, "BGP Prefix Origin Validation," P. Mohapatra, et al., January 2013

[RFC 7115] IETF RFC 7115, "Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)," R. Bush, January 2014

[RFC 7646] IETF RFC 7646, “Definition and Use of DNSSEC Negative Trust Anchors”, P. Ebersman, W. Kumari, C. Griffiths, J. Livingood, R. Weber, September 2015

[RFC 7454] IETF RFC 7454, "BGP Operations and Security," J. Durand, I. Pepelnjak, G. Doering, February 2015

[RFC 7908] IETF RFC 7908, "Problem Definition and Classification of BGP Route Leaks," K. Sriram, D. Montgomery, D. McPherson, E. Osterweil, B. Dickson, June 2016

[RFC 8183] IETF RFC 8183, “An Out-of-Band Setup Protocol for Resource Public Key Infrastructure (RPKI) Production Services”, R. Austein, July 2017

[RFC 8446] IETF RFC 8446, "The Transport Layer Security (TLS) Protocol Version 1.3," E. Rescorla, August 2018

[RFC 9234] IETF RFC 9234, “Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages”, A. Azimov, E. Bogomazov, R. Bush, K. Patel, K. Sriram, May 2022

[RFC 9319] IETF RFC 9319, "The Use of maxLength in the Resource Public Key Infrastructure (RPKI)," Y. Gilad, S. Goldberg, K. Sriram, J. Snijders, B. Maddison, October 2022

[RPKI-BCP] Resource Public Key Infrastructure (RPKI) Deployment Best Common Practice, CL-GL-RPKI-BCP-V01-220120, January 20, 2022, Cable Television Laboratories, Inc.

2.2 Further Reading

Broadband Internet Technical Advisory Group (BITAG), "Security of the Internet Routing Infrastructure," Technical Working Group Report, November 2022, https://www.bitag.org/documents/BITAG_Routing_Security.pdf

IETF RFC 2827 (BCP 38), "Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing," P. Ferguson, D. Senie, May 2000

IETF RFC 3013 (BCP 46), "Recommended Internet Service Provider Security Services and Procedures," T. Killalea, November 2000

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone: +1-303-661-9100; Fax: +1-303-661-9199; http://www.cablelabs.com
- IETF: Internet Engineering Task Force Secretariat, c/o Association Management Solutions, LLC (AMS), Fremont, CA 94538; Phone: +1-510-492-4080, Fax: +1-510-492-4001; http://www.ietf.org
- National Institute of Standards and Technology; https://www.nist.gov

3 ABBREVIATIONS

This guideline uses the following abbreviations.

ACL	access control list
AS	autonomous system
ASN	autonomous system number
BGP	Border Gateway Protocol
CA	certificate authority
CPU	central processing unit
CSF	NIST Cybersecurity Framework
CSP	cloud service providers
DDoS	distributed denial of service
DNS	domain name services
FIB	forwarding information base
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IRR	Internet Routing Registry
ISP	internet service provider
IT	information technology
NIST	National Institute of Standards and Technology
OAM	operations, administration, and management
RIR	Regional Internet Registry
ROA	route origin authorization
ROV	route origin validation
RP	relying party
RPKI	resource public key infrastructure
RRDP	RPKI Repository Delta Protocol
RSYNC	remote sync
RTR	RPKI to router
SCRM	supply chain risk management
SSH	Secure Shell Protocol
TLS	transport layer security

4 OVERVIEW

This section provides an overview of routing security and outlines how the profile leverages the NIST Cybersecurity Framework (CSF) (https://www.nist.gov/cyberframework) for specialized guidance. The CSF provides a common set of categories and subcategories that organize cybersecurity activities into functions: Govern, Identify, Protect, Detect, Respond, and Recover [NIST CSF 2.0].

This routing security profile customizes the CSF structure by mapping routing security best practices to the applicable categories and subcategories. In this way, the routing security profile aims to serve as an informative reference for standards, guidelines, and best practices related to routing security.

4.1 Routing Security Overview

This section provides a brief overview of the technologies related to internet routing security, such as BGP, IRRs, AS path filtering, and RPKI (including ROA and ROV).

Border Gateway Protocol (BGP)—BGP is the predominant protocol used for routing between organizations. BGP enables networks under different administrative control to exchange routing information through configured peering relationships. This allows each network to learn routes to prefixes (blocks of IP addresses) originating from its BGP neighbors. BGP speakers, routers that run BGP, make routing decisions based on policies to determine optimal paths for traffic flow between autonomous systems. Securing BGP is crucial for ensuring reliable connectivity across networks.

Internet Routing Registries (IRRs)—IRRs are databases for sharing routing policy information between network operators. Other operators can then query an IRR to retrieve routing policy data to create route filters and ACLs (e.g., source address validation on incoming IP packets) (Figure 2). Historically, IRRs have had limitations—they contain uncontrolled self-published data of varying quality and sometimes lack rigorous approaches to authentication and authorization. As a result, newer technologies like RPKI have been designed to try to address these weaknesses. If IRRs are to be used, one needs to consider the authorization model of the IRR data and should also consider using RPKI to cross check IRR data for consistency.

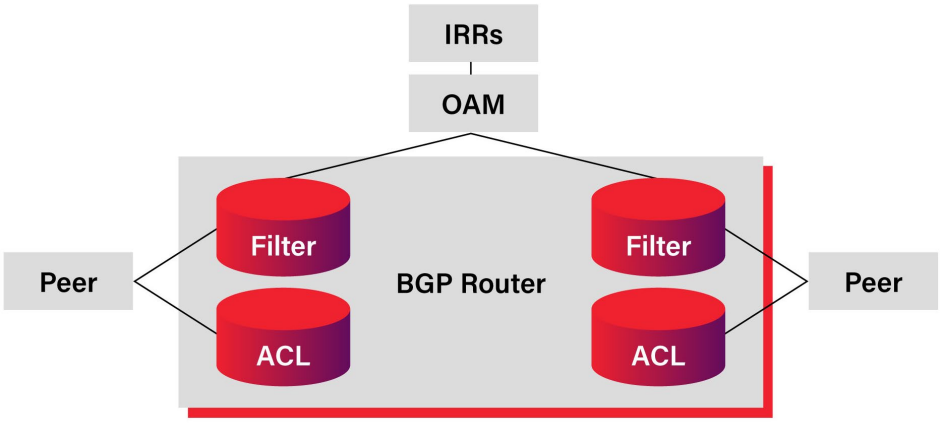

Figure 2 - IRR Used to Facilitate Route and Packet Filtering

Autonomous system (AS) path filtering—AS path filtering is a technique used between BGP routers to improve routing security by inspecting the AS path attribute and selectively blocking invalid or unintended routes. For example, filters can reject routes containing well-known transit AS numbers (ASNs) to prevent accidental route leaks to neighbors [RFC 7908]. This prevents propagation of unintended paths by rejecting routes that contain unauthorized autonomous systems. AS path filtering requires coordination between networks, so misconfigurations could impact reachability. However, when applied correctly, AS path filters are a powerful tool to improve routing security.

Resource public key infrastructure (RPKI)—RPKI [RFC 6480] is a special-purpose public key certificate infrastructure and publication system designed to support BGP security (Figure 3). RPKI creates a trusted linkage between routing resources and the entities authorized to describe the intended use of those resources. Route origin validation (ROV) is the first application of the RPKI system. By publishing route origin authorization (ROA) objects, an IP address holder can attest to the autonomous systems that are authorized to originate routes for a given set of IP addresses into the global BGP routing system. This approach helps lessen the risk of accidental or malicious route leaks or mis-originations ("hijacks").

Route origin authorizations (ROAs)—A ROA is a digitally signed object that authorizes a specific AS to announce in BGP-specific IP address blocks.

Route origin validation (ROV)—ROV enables verification that the BGP route announcements match the ASN specified in the corresponding ROA. This prevents some, albeit not all, route hijacking and invalid route announcements by ensuring prefixes are announced only by authorized networks.

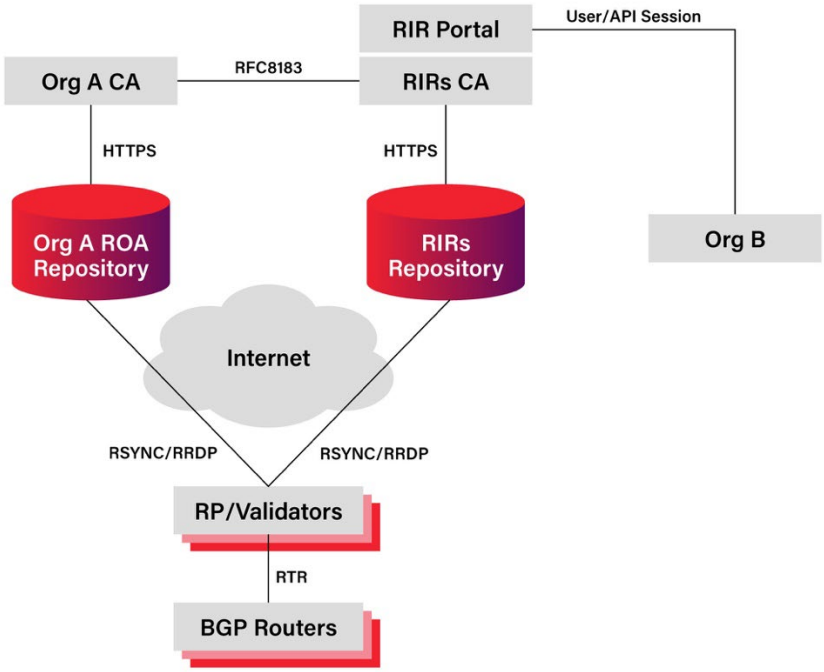

Figure 3 - RPKI Architecture

As depicted above, many parties are involved in routing security, including routing peers, IRR, and RIRs, among others. From a cybersecurity perspective, an organization needs to engage with those external entities or stakeholders to ensure the security of internet routing. Routing stakeholders can be classified into three categories, including suppliers (e.g., hardware, software, and outsourced service vendors, upstream providers, RIRs, IRRs, Internet eXchanges, open source software developers), customers (e.g., downstream networks), and other interconnection partners.

4.2 Cybersecurity Framework Overview

The NIST Cybersecurity Framework [NIST CSF 2.0] consists of three main components.

- The CSF Core provides a set of cybersecurity activities, desired outcomes, and references that are common across critical infrastructure sectors that can help an organization manage its cybersecurity risk.

- The CSF Tiers provide context on how an organization views cybersecurity risk and the process in place to manage the risk in a progressive manner from Tier 1 (Partial) to Tier 4 (Adaptive). They can be applied to CSF Organization Profiles to "characterize the rigor of an organization's cybersecurity risk governance and management practices." [NIST CSF 2.0]
- The CSF Organizational Profiles can be considered as the alignment of standards, guidelines, and practices to the CSF Core in a particular implementation scenario. They are a "mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes." A Community Profile is a baseline of CSF outcomes typically developed for a particular sector, subsector, technology, threat type, or other use case to address shared interests and goals across organizations [NIST CSF 2.0].

The CSF Core consists of three hierarchal components: functions, categories, and subcategories. At the highest level are functions: Govern, Identify, Protect, Detect, Respond, and Recover. These functions relate to one another and should be addressed concurrently. Categories are subdivisions of a function, and subcategories further divide categories into specific outcomes.

The six functions are briefly described below [NIST CSF 2.0].

1. Govern—Establish, communicate, and monitor the organization's cybersecurity risk management strategy, expectations, and policy.
2. Identify—Understand the organization's current cybersecurity risks.
3. Protect—Use safeguards to manage the organization's cybersecurity risks.
4. Detect—Find and analyze possible cybersecurity attacks and compromises.
5. Respond—Take actions regarding a detected cybersecurity incident.
6. Recover—Restore assets and operations affected by a cybersecurity incident.

5 ROUTING SECURITY PROFILE

This routing security profile section was created using the Cybersecurity Framework 2.0, as described in Section 4.2. Each subsection of this section corresponds to a CSF core function, which is further divided into categories and subcategories. For each category, a table lists the subcategories and their applicability to routing security.

By design, the cybersecurity framework is inherently flexible to accommodate different organizations' unique environments and needs. Organizations and BGP practitioners are advised to review all subcategories in the context of their organization and follow the recommendations as needed.

5.1 Govern

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

The Govern (GV) function defines six categories.

- Organizational Context (GV.OC)
- Risk Management Strategy (GV.RM)
- Roles, Responsibilities, and Authorities (GV.RR)
- Policy (GV.PO)
- Oversight (GV.OV)
- Cybersecurity Supply Chain Risk Management (GV.SC)

Within these broad categories, all subcategories generally apply to routing security. In some cases, there may be no specifically applicable considerations for routing security.

5.1.1 Govern: Organizational Context (GV.OC)

The circumstances—mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements—surrounding the organization's cybersecurity risk management decisions are understood.

In internet routing, it is critical to understand the responsibilities and expectations of both internal and external routing stakeholders, including but not limited to, routing vendors, upstream providers, RIRs, IRRs, Internet eXchanges, interconnection partners, and customers.

The "Govern: Organizational Context" category has five subcategories, all of which apply to routing security except one without routing specific considerations.

Table 1 - Govern: Organizational Context (GV.OC)

Subcategory	Applicability to Internet Routing
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management.	Applicable, no routing-specific considerations
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered.	Internal and external routing stakeholders are understood, and their needs, roles, and expectations regarding routing security risk management are understood and considered. Routing stakeholders include suppliers (e.g., vendors, upstream providers, RIRs, IRRs, Internet eXchanges), customers (e.g., downstream networks), and other interconnection partners.
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—are understood and managed.	National and regional legal and regulatory requirements and BGP peering contractual requirements regarding routing security are understood and managed.

Subcategory	Applicability to Internet Routing
GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.	Critical objectives, capabilities, and services that external routing stakeholders depend on or expect from the routing engineering team in the organization are understood and communicated. For example, external stakeholders may expect the organization to maintain accurate routing registration information (e.g., in IRR) so they can build routing filter rules properly. For another example, an external stakeholder, e.g., an IP transit provider for the organization, depends on the organization to create ROAs for the address spaces that are owned by the organization but are originated by the external stakeholder.
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated.	Outcomes, capabilities, and services that the routing and security teams (e.g., routing engineer, RPKI team, cybersecurity team) in the organization depend on are understood and communicated.

5.1.2 Govern: Risk Management Strategy (GV.RM)

The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.

In internet routing, an important part of risk management strategy involves the understanding of routing security risks, such as risks from RIRs, routing software and hardware vendors, routing tools, and downstream and upstream routing peers. Particularly, risks (e.g., vulnerabilities) from critical routing software and tools from open sources need to be communicated and understood across the organization.

The "Govern: Risk Management Strategy" category has seven subcategories, all of which apply to routing security.

Table 2 - Govern: Risk Management Strategy (GV.RM)

Subcategory	Applicability to Internet Routing
GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders.	Risk management objectives related to routing, including routing infrastructure, routing security infrastructure such as RPKI, and supporting infrastructure such as OAM, are established and agreed to by the routing engineering and cybersecurity teams.
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained.	Risk appetite and risk tolerance statements related to routing, routing security, and supporting infrastructure are established, communicated, and maintained.
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.	Cybersecurity risk management activities and outcomes related to routing are included in the organization's risk management processes.
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated.	Strategic direction that describes appropriate risk response options related to routing incidents is established and communicated.
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.	Lines of communication across the organization are established for routing security risks, including risks from RIRs, routing software and hardware vendors, routing tools, and downstream and upstream routing peers. Particularly, risks (e.g., vulnerabilities) from critical software and tools from open sources are communicated and understood.
GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.	A method for calculating, documenting, categorizing, and prioritizing routing security risks (such as routing hijacking, routing leaks, invalid ROAs) is established and communicated.
GV.RM-07: Strategic opportunities (e.g., positive risks) are characterized and are included in organizational cybersecurity risk discussions.	In routing, interconnection opportunities can be leveraged to improve routing service availability. New technologies for enhancing routing security should be monitored and discussed.

5.1.3 Govern: Roles, Responsibilities, and Authorities (GV.RR)

Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.

Roles and responsibilities related to internet routing are often divided and shared among different teams. For example, the team that is responsible for RPKI may not be the same team responsible for the operation of routing. It is important to make sure roles and responsibilities related to routing security are established and understood.

The "Govern: Roles, Responsibilities, and Authorities" category has four subcategories, all of which apply to routing security, with two without routing specific considerations.

Table 3 - Govern: Roles, Responsibilities, and Authorities (GV.RR)

Subcategory	Applicability to Internet Routing
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.	Applicable, no routing-specific considerations.
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.	Roles, responsibilities, and authorities related to routing security risk management are established, communicated, understood, and enforced. Particularly, contacts with external routing stakeholders are established and expectations to and from them are communicated and understood. Communications received from external stakeholders and other parties (e.g., security researchers) are also treated carefully to understand potential risks to the organization's own networks.
GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.	Adequate resources, including personnel, training, and funding, are allocated commensurate with the routing security risk strategy, roles, responsibilities, and policies.
GV.RR-04: Cybersecurity is included in human resources practices.	Applicable, no routing-specific considerations.

5.1.4 Govern: Policy (GV.PO)

Organizational cybersecurity policy is established, communicated, and enforced. For internet routing, regulatory policy related to routing security may need to be taken into consideration.

The "Govern: Policy" category has two subcategories, both of which apply to routing security.

Table 4 - Govern: Policy (GV.PO)

Subcategory	Applicability to Internet Routing
GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	Policy for managing routing security risks, by taking into consideration regulatory routing security requirements, is established, communicated, and enforced.
GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	Policy for managing routing security risks is reviewed, updated, communicated, and enforced on a regular basis to reflect changes in requirements, including regulatory requirements, threats, technology, organizational changes (including acquisitions), and organizational mission.

5.1.5 Govern: Oversight (GV.OV)

Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.

The "Govern: Oversight" category has three subcategories, all of which apply to routing security without routing specific considerations.

Table 5 - Govern: Oversight (GV.OV)

Subcategory	Applicability to Internet Routing
GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	Applicable, no routing-specific considerations.
GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.	Applicable, no routing-specific considerations.
GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.	Applicable, no routing-specific considerations.

5.1.6 Govern: Cybersecurity Supply Chain Risk Management (GV.SC)

Cybersecurity supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.

Supply chain of internet routing involves many parties, including IRRs, RIRs, routing hardware and software vendors, upstream providers, downstream customers, and interconnect partners. Risks from each involved party need to be analyzed and understood.

The "Govern: Cybersecurity Supply Chain Risk Management" category has ten subcategories, all of which apply to routing security, with two without routing specific considerations.

Table 6 - Govern: Cybersecurity Supply Chain Risk Management (GV.SC)

Subcategory	Applicability to Internet Routing
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.	Applicable, with specific consideration of routing supply chain, including IRRs, RIRs, ROAs, ROA repositories, ROV validators, and routing software and hardware, among others. Particularly, risks from accounts and credentials for IRRs and RIRs need to be considered and mitigated.
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.	Routing security roles and responsibilities for internal routing stakeholders (e.g., routing engineering, routing operations, IRR data management, ROA management, etc.) and external stakeholders, including suppliers (e.g., software and hardware vendors, upstream providers), customers (e.g., downstream customers), and interconnect partners, are established, communicated, and coordinated internally and externally.
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.	Risk management for the routing supply chain is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement process.

Subcategory	Applicability to Internet Routing
GV.SC-04: Suppliers are known and prioritized by criticality.	Suppliers for routing infrastructure (e.g., router vendors, routing interconnect partners), routing security infrastructure such as RPKI (e.g., RIRs, ROV validators), and routing supporting infrastructure (e.g., OAM vendors, IRRs, outsourced partners), are known and prioritized by criticality.
GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.	Applicable with specific consideration of routing supply chain security requirements. For example, a requirement may be included in a contract with a router vendor to monitor and respond to vulnerabilities reported by customers or third parties affecting their products and/or services.
GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.	Applicable with specific consideration of reducing risks from routing suppliers. For example, before entering into a formal relationship, study the reputation and records of the routing suppliers in handling reported vulnerabilities affecting their products and/or services.
GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship.	Applicable with specific consideration of risks posed by a routing supplier, such as software and hardware supplier (e.g., a router vendor, ROV validator supplier) and routing service suppliers (e.g., IRRs, RIRs, upstream service providers, interconnect service providers).
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.	Applicable with specific consideration of routing suppliers (see above), with understanding that some suppliers (e.g., open-source components without formal support) may not be able to be included in the incident planning, response, and recovery activities.
GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle.	Applicable, no routing-specific considerations.
GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.	Applicable, no routing-specific considerations.

5.2 Identify

The organization's current cybersecurity risks are understood.

The Identify (ID) function defines three categories:

- Asset Management (AM),
- Risk Assessment (RA), and
- Improvement (IM).

Within the three categories, all subcategories apply to routing security.

5.2.1 Identify: Asset Management (ID.AM)

Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

In the context of routing security, organizations need to inventory internal and external routing services, routing devices and related computing devices, and their configurations. Working knowledge of the interfaces and data flows between devices and organizations, respectively, will illuminate areas of risk and needed protective measures.

The "Identify: Asset Management" category has seven subcategories, all of which apply to routing security.

Table 7 - Identify: Asset Management (ID.AM)

Subcategory	Applicability to Internet Routing
ID.AM-01: Inventories of hardware managed by the organization are maintained.	Routing hardware should be inventoried, including BGP routers and computing devices used for RPKI and management functions.
ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.	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 those used for RPKI certificate authority.
ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained.	Routing information such as policies, filters, ACLs, routes, etc., should be maintained to facilitate understanding of what information needs to be protected, who has access, and why.
ID.AM-04: Inventories of services provided by suppliers are maintained.	Inventories of routing services provided by suppliers are maintained, such as routing peers, IRRs, RIRs, and routing monitoring service providers. Inventories of other outsourced critical IT services interdependent with routing services are also maintained, such as outsourced email, DNS, storage, CSPs, etc. Examples include master service agreements (MSAs) and/or other contracts with vendors and suppliers. These are not only applied to providers of routing and other infrastructure hardware and software, but also services such as registries, monitoring and analysis systems, etc.
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission.	Routing-related assets, including hardware, software, services, and systems, are prioritized based on their classification, criticality, resources, and impact on internet routing and routing security. For providers of networking or network-based services (including internet access or other connectivity, cloud computing, software as a service (SaaS)), consider criticality of not only revenue-generating assets but also internal-facing components that provide billing, customer records, continuity, and HR and internal services.
ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained.	Applicable with specific consideration of routing-related data such as routing filters, ACLs, IRR data, ROAs, etc.
ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles.	Routing-related systems, hardware, software, services, and data are managed throughout their life cycles. For example, ROAs need to be issued for address spaces that are in use and removed timely when the protected address space is not in use anymore. Routing data in IRRs should also be added, updated, and deleted timely to prevent incorrect and stale data.

5.2.2 Identify: Risk Assessment (ID.RA)

The cybersecurity risk to the organization, assets, and individuals is understood by the organization.

The routing elements may have varying risk tolerance levels, and the routing system may inherit a level of risk from its partners or other components of the routing system that exceeds its risk tolerance. Identify cyber risks associated with external service providers and their components as they relate to the overall risk management strategy.

The "Identify: Risk Assessment" category has ten subcategories, all of which apply to routing security.

Table 8 - Identify: Risk Assessment (ID.RA)

Subcategory	Applicability to Internet Routing
ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded.	Vulnerabilities in routing assets, including routing protocols (e.g., [RFC 4272]), hardware, software, and services are identified, validated, and recorded. Particular attention needs to be paid to vulnerabilities in routing assets that are based on open source components, such as RPKI validator software and routing software.
ID.RA-02: Cyber threat intelligence is received from information-sharing forums and sources.	Cyber threat intelligence on internet routing is received from information-sharing forums and sources that may be either closed (e.g., for a particular routing community) or open to the public. The organization is encouraged to participate and contribute to cyber threat intelligence information-sharing forums and activities.
ID.RA-03: Internal and external threats to the organization are identified and recorded.	Internal and external threats to internet routing are identified and recorded. Internal threats such as insider attacks resulting from the ability to reconfigure, compromise, or damage routing infrastructure but also threats to the organization's accounts in RIRs are identified and recorded because an adversary could use the compromised RIR account to issue malicious ROAs to invalidate the routes originated by the organization or to hijack the organization's address space. For another example, threats to an organization's outsourced critical functions are also identified and recorded.
ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.	Applicable, with specific consideration of potential impacts and likelihoods of threats exploiting vulnerabilities in routing assets. For example, how likely can a vulnerability in a BGP speaker be remotely exploited? Does a vulnerable BGP speaker reject packets from a remote entity on the internet that is not a direct peer (e.g., two or more hops away)?
ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.	Applicable with specific consideration on threats of high risk (e.g., compromised RIR account) to internet routing, even though the likelihood of such threat may be low.
ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated.	Applicable with specific consideration on responses to threats of high risk (e.g., compromised RIR account) to internet routing.
ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.	Applicable with specific consideration of changes and exceptions to routing engineering practices. For example, if some more specific prefixes are advertised to a direct neighbor (with non-export BGP attribute), e.g., for traffic engineering purposes, ROAs for those more specific prefixes are not needed and may be even harmful since they can be misused by an adversary to facilitate prefix hijacking (e.g., by additionally manipulating AS-PATH).
ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established.	Applicable with specific consideration on the processes for interacting with external routing stakeholders (e.g., router vendors) in responding to vulnerability disclosures.
ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use.	Applicable with specific consideration on the authenticity and integrity of routing-related hardware and software, including open source based and where there is no contractual agreement with the suppliers.
ID.RA-10: Critical suppliers are assessed prior to acquisition.	Applicable with specific consideration of the security posture of critical routing suppliers, e.g., if they have established a security incident response process.

5.2.3 Identify: Improvement (ID.IM)

Improvements to organizational cybersecurity risk management processes, procedures, and activities are identified across all CSF functions.

In internet routing, areas for improvement can be identified and executed by evaluating external routing reporting services, security testing, and incident responses, among other procedures.

The "Identify: Improvement" category has four subcategories, all of which apply to routing security.

Table 9 - Identify: Improvement (ID.IM)

Subcategory	Applicability to Internet Routing
ID.IM-01: Improvements are identified from evaluations.	Improvements to internet routing security are identified from evaluations. For example, by evaluating external RPKI reporting services (e.g., NIST RPKI Monitor), an organization may create new ROAs for its announced address spaces that are currently in unknown state or invalid state.
ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties.	Applicable with specific consideration on improvement of routing configuration, filtering, and hardening. For example, if an external audit discovers some ports are open and accessible on a router, the issue should be remediated properly.
ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities.	Improvements to internet routing and routing security are identified from execution of operational processes, procedures, and activities such as analysis of routing events and alerts.
ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.	Incident response plans that affect internet routing and routing security are established, communicated, maintained, and improved.

5.3 Protect

Safeguards to manage the organization's cybersecurity risks are used.

The Protect (PR) function defines five categories:

- Identity Management, Authentication, and Access Control (PR.AA),
- Awareness and Training (PR.AT),
- Data Security (PR.DS),
- Platform Security (PR.PS), and
- Technology Infrastructure Resilience (PR.IR).

All subcategories in the five categories apply to routing security.

5.3.1 Protect: Identity Management, Authentication, and Access Control (PR.AA)

The "Protect: Identity Management, Authentications, and Access Control" category has six subcategories, all of which apply to routing security.

Table 10 - Protect: Identity Management, Authentication, and Access Control (PR.AA)

Subcategory	Applicability to Internet Routing
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization.	Identities and credentials for routing devices are issued, managed, verified, revoked, and audited for authorized devices, users, and processes. Identities and credentials for external accounts, e.g., RIR accounts, need to be managed with special care because of the potential impact to internet routing from such compromised accounts.

Subcategory	Applicability to Internet Routing
PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions.	Applicable with specific consideration of routing-related identities and credentials.
PR.AA-03: Users, services, and hardware are authenticated.	Applicable with specific consideration of routing-related users, services, and hardware, including • user access to routing devices and systems containing routing information; and • services containing routing-related information such as IRR, RIR, and peeringDB.
PR.AA-04: Identity assertions are protected, conveyed, and verified.	Applicable with specific consideration of routing-related identities for the local and peer networks.
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed and incorporate the principles of least privilege and separation of duties.	Access permissions, entitlements, and authorizations policy should cover • routing devices, • automation systems, and • databases containing routing-related information. Policies should be reviewed regularly.
PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk.	Physical access should be managed, monitored, and enforced for routing devices, systems that manage routers, credential stores with routing related credentials, and any backups.

5.3.2 Protect: Awareness and Training (PR.AT)

The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks.

In internet routing, training should be provided to specialized engineers responsible for routing infrastructure on routing security technologies and best common practices.

The "Protect: Awareness and Training" category has two subcategories, both of which apply to routing security.

Table 11 - Protect: Awareness and Training (PR.AT)

Subcategory	Applicability to Internet Routing
PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.	General awareness of risks to routing security (e.g., impact on DNS) and routing dependencies such as IRR and RPKI systems should be included in training for appropriate personnel.
PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind.	Routing engineers are provided with awareness and training related to routing security such as route filtering, RPKI, IRR, etc., so they can implement relevant best common practices to improve routing security.

5.3.3 Protect: Data Security (PR.DS)

Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

In internet routing, confidentiality of routing policy information (e.g., ROAs), while important, is usually of less concern, but integrity and availability are of critical importance.

The "Protect: Data Security" category has four subcategories, all of which apply to routing security.

Table 12 - Protect: Data Security (PR.DS)

Subcategory	Applicability to Internet Routing
PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected.	Data at rest, such as device and system configuration and configuration templates, are maintained to ensure integrity and availability. Where appropriate, confidentiality of keying materials (e.g., encryption and integrity keys) is also protected. Make sure ROAs remain valid (e.g., not expired). Ensure diversity and availability of RPKI validating caches for use by routing infrastructure for ROV.
PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.	The routing infrastructure's in-band and out-of-band (OOB) communications are protected (see BGP OpsSec [RFC 7454]). Check for shared fate of OOB access to persist in case of routing system disruption. Administrative sessions from management stations to BGP routers need to be protected, e.g., by using SSH [RFC 4253] or TLS [RFC 8446]. RPKI ROV can be deployed to ensure that prefixes originated in a BGP update by the origin AS are authorized. Methods such as control-plane ACLs and rate-limiting and/or GTSM or TCP-AO can help protect the router's BGP process remain available and to lessen the risk of interruption of BGP message exchange.
PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected.	Confidentiality of routing information is generally not a concern for global routing. Filtering should be applied on BGP sessions to ensure routing integrity. Redundancy should be implemented for availability. This may require detailed planning with routing partners.
PR.DS-11: Backups of data are created, protected, maintained, and tested.	Backups and restoration for routing device configuration and all support systems should be maintained and periodically tested.

5.3.4 Protect: Platform Security (PR.PS)

The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.

In internet routing, change management processes are important for managing changes for device configuration, software/firmware, and hardware.

The "Protect: Platform Security" category has six subcategories, all of which apply to routing security.

Table 13 - Protect: Platform Security (PR.PS)

Subcategory	Applicability to Internet Routing
PR.PS-01: Configuration management practices are established and applied.	Establish and document change management processes for network topology changes, prefix announcement changes, network policy changes, and peering relationship changes.
PR.PS-02: Software is maintained, replaced, and removed commensurate with risk.	Ensure that routing-related software, e.g., router operating systems, software routing packages, and RPKI validator, is maintained, replaced, and removed commensurate with risk.

Subcategory	Applicability to Internet Routing
PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk.	Routing-related hardware, e.g., routers, is maintained, replaced, and removed commensurate with risk.
PR.PS-04: Log records are generated and made available for continuous monitoring.	Device logs are generated and maintained for monitoring and analysis. It may also be useful to periodically dump RIBs, unselected routes, or filtered routes.
PR.PS-05: Installation and execution of unauthorized software are prevented.	This has not been a common attack vector for routing. However, if general-purpose platforms (e.g., Unix devices) are used for routing, some review and validation of approved software packages should be implemented.
PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle.	Secure software development practices should be used for internally developed software. Notifications provided for externally developed software should be monitored. It is particularly important that unexpected inputs (e.g., uncommon or poorly formed BGP attributes) are handled appropriately.

5.3.5 Protect: Technology Infrastructure Resilience (PR.IR)

Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience.

In the context of internet routing, this category relates to the organization's enterprise network to support operations and management of routing infrastructure. It is vital that the availability of the network to support these functions be maintained, particularly in the face of possible routing instability such that staff can maintain control of the infrastructure in order to address problems (e.g., outages or attacks). Particularly, it is important to consider the reliance (fate sharing) of these networks on the internet underlay, for instance in the case of remote access such as using VPNs or other cloud services, authentication, DNS, etc.

The "Protect: Technology Infrastructure Resilience" category has four subcategories, all of which apply to routing security.

Table 14 - Protect: Technology Infrastructure Resilience (PR.IR)

Subcategory	Applicability to Internet Routing
PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	Routing environments (e.g., routers and OAM systems) are protected from unauthorized logical access (e.g., remote access) and usage.
PR.IR-02: The organization's technology assets are protected from environmental threats.	Routing hardware deployed outside climate-controlled environments requires special consideration to ensure continuous operation.
PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	Resiliency planning with network peers is generally required to ensure continuous operation in the face of device or infrastructure failures. Resiliency is an important consideration for the continuous operation of internal systems. It is important to have a thorough understanding of dependencies between systems. Additionally, reliance on other systems (e.g., RPKI infrastructure) should also be considered in the face of various failure modes.
PR.IR-04: Adequate resource capacity to ensure availability is maintained.	Capacity planning with network peers is generally required to ensure continuous operation in the face of device or infrastructure failures. Adequate capacity of routing devices (routing tables, ACLs, ports, links, router CPU, etc.) and routing support systems (CPU, memory, network capacity) is maintained to ensure availability.

5.4 Detect

Possible cybersecurity attacks and compromises are found and analyzed.

The Detect (DE) function defines three categories:

- Anomalies and Event (AE),
- Security Continuous Monitoring (CM), and
- Detection Processes (DP).

All subcategories in the three categories apply to routing security.

5.4.1 Detect: Continuous Monitoring (DE.CM)

Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.

In an internet routing network environment, it is critical to classify the routing relationship with all BGP peers, which will determine routing policies toward each peer. The routing relationship and routing and filtering policies toward each peer form the baseline of the network operations, which can be used to deploy and maintain anomaly detection and continuous monitoring.

The "Detect: Continuous Monitoring" category has five subcategories, all of which apply to routing security.

Table 15 - Detect: Continuous Monitoring (DE.CM)

Subcategory	Applicability to Internet Routing
DE.CM-01: Networks and network services are monitored to find potentially adverse events.	A classification of relationships with BGP peers (e.g., as transit provider, customer, or peer) is established. A baseline of routes and traffic expected from each BGP peer is established. Validation and filtering and policy are established and managed. Routing networks and assets (ROA repositories, ROV infrastructure), including external networks such as global routing, are monitored continuously.
DE.CM-02: The physical environment is monitored to find potentially adverse events.	Physical environment for routing equipment, including on-premise and shared environment (e.g., cloud provider and IP exchange), are monitored, e.g., for physical access and environmental conditions.
DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events.	Physical and remote access to and usage of the routing environment, including configuration and management systems, are monitored and managed based on roles and responsibilities.
DE.CM-06: External service provider activities and services are monitored to find potentially adverse events.	External routing service provider activities and services, such as RIR and IRR, are monitored, e.g., for unauthorized changes to routing policy information.
DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.	Routing hardware and software are monitored for abnormalities (e.g., high CPU, memory usage, crashes). Routing advertisements are monitored, e.g., for route leaks or hijacking.

5.4.2 Detect: Adverse Event Analysis (DE.AE)

Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.

In the context of internet routing, analysis of routing incidents needs to take into consideration information from multiple sources, e.g., from internal and external stakeholders and data sources, as well as cyber threat intelligence and other contextual information, e.g., ongoing regional or global events that may have an impact on routing.

The "Detect: Adverse Event Analysis" category has six subcategories, all of which apply to routing security.

Table 16 - Detect: Adverse Event Analysis (DE.AE)

Subcategory	Applicability to Internet Routing
DE.AE-02: Potentially adverse events are analyzed to better understand associated activities.	Upon detecting abnormal routing events, discuss internally and externally to understand potential activities that may have caused the events.
DE.AE-03: Information is correlated from multiple sources.	Information from multiple sources, e.g., from internal and external stakeholders, is collected and correlated to facilitate the analysis of scope and impact.
DE.AE-04: The estimated impact and scope of adverse events are understood.	Impact and scope of a routing incident is estimated and understood, with a general understanding that routing incidents often have a high impact on customers and the internet in general.
DE.AE-06: Information on adverse events is provided to authorized staff and tools.	Information on routing incidents is provided to authorized staff (both internal and external) and tools.
DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis.	Analysis of routing incidents need to take into consideration cyber threat intelligence and other contextual information, e.g., ongoing regional or global events that may have an impact on routing.
DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria.	Routing incidents are declared and shared with authorized parties when meeting the defined incident criteria.

5.5 Respond

Actions regarding a detected cybersecurity incident are taken.

The Respond (RS) function defines four categories:

- Incident Management (RS.MA),
- Incident Analysis (RS.AN),
- Incident Response Reporting and Communication (RS.CO), and
- Incident Mitigation (RS.MI).

All subcategories in each of the four categories apply to internet routing.

5.5.1 Respond: Incident Management (RS.MA)

Responses to detected cybersecurity incidents are managed.

Incident response for internet routing needs to be coordinated with routing stakeholders, e.g., upstream service providers, IP interconnection partners, and customers.

The "Respond: Incident Management" category has five subcategories, all of which apply to routing security.

Table 17 - Respond: Incident Management (RS.MA)

Subcategory	Applicability to Internet Routing
RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared.	Incident response plan for routing is executed in coordination with routing stakeholders, e.g., upstream service providers, IP interconnection partners, and customers.
RS.MA-02: Incident reports are triaged and validated.	Routing incident reports are triaged and validated.
RS.MA-03: Incidents are categorized and prioritized.	Routing incidents are categorized and prioritized based on their scope, impact, and potential causes.

Subcategory	Applicability to Internet Routing
RS.MA-04: Incidents are escalated or elevated as needed.	Routing incidents are escalated or elevated as needed, e.g., for those with a high impact on customers and global routing.
RS.MA-05: The criteria for initiating incident recovery are applied.	The criteria for initiating incident recovery from routing incidents are applied. In general, a routing incident that may result in service outage needs to be recovered as quickly as possible.

5.5.2 Respond: Incident Analysis (RS.AN)

Investigations are conducted to ensure effective response and support forensics and recovery activities.

Analysis of a routing incident is conducted to understand the root cause, e.g., buggy software upgrades or patches, misconfiguration, external propagation, malicious hijacking.

The "Respond: Incident Analysis" category has four subcategories, all of which apply to routing security.

Table 18 - Respond: Incident Analysis (RS.AN)

Subcategory	Applicability to Internet Routing
RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident.	Analysis of a routing incident is performed to understand the root cause, e.g., buggy software patches, misconfiguration, external propagation, malicious hijacking.
RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved.	Applicable, no routing-specific considerations.
RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved.	Routing incident data may pertain, e.g., incidental routing updates and erroneous ROAs, are collected and their integrity and provenance are preserved.
RS.AN-08: An incident's magnitude is estimated and validated.	The impact of a routing incident is estimated and validated, e.g., by correlating time frames across both control plane and data plane information.

5.5.3 Respond: Incident Response Reporting and Communication (RS.CO)

Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies.

The "Respond: Incident Response Reporting and Communication" category has two subcategories, both of which apply to routing security.

Table 19 - Respond: Incident Response Reporting and Communication (RS.CO)

Subcategory	Applicability to Internet Routing
RS.CO-02: Internal and external stakeholders are notified of incidents.	Internal and external routing stakeholders that are relevant to the routing incidents, e.g., customers, upstream providers, etc., are notified of the incidents in alignment with broader organizational policies.
RS.CO-03: Information is shared with designated internal and external stakeholders.	Information about the routing incidents, including technical information, is shared with designated internal and external routing stakeholders, e.g., customers, upstream providers, etc., in alignment with broader organizational policies.

5.5.4 Respond: Incident Mitigation (RS.MI)

Activities are performed to prevent expansion of an event and mitigate its effects.

The "Respond: Incident Mitigation" category has two subcategories, both of which apply to routing security.

Table 20 - Respond: Incident Mitigation (RS.MI)

Subcategory	Applicability to Internet Routing
RS.MI-01: Incidents are contained.	Routing incidents are contained to prevent them from further propagating. Depending on the incidents, new RPKI-ROAs are created, and RPKI-ROV filtering is deployed as appropriate. Invalid routes are dropped and the peer ASN that transmitted them are notified. Filtering policies are reviewed and adjusted as needed.
RS.MI-02: Incidents are eradicated.	Root cause of the routing incident is understood and remediated. For example, a routing misconfiguration that results in the incident is corrected. If the routing incident is caused by an external event, the offending ASs and their upstream providers may be contacted, if possible, to address the incidents, e.g., by correcting their misconfiguration. Review mitigating routing policy in place and adjust accordingly.

5.6 Recover

Assets and operations affected by a cybersecurity incident are restored.

The Recover (RC) function defines three categories:

- Recovery Planning (RP),
- Improvements (IM), and
- Communication (CO).

Within the three categories, all subcategories generally apply to routing security. In some cases, there may be no specifically applicable considerations for routing security.

5.6.1 Recover: Incident Recovery Plan Execution (RC.RP)

Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents.

Recovery from routing incidents often involves adjustment of routing configurations and/or policies (e.g., route filtering, ACLs) and/or other parameters.

The "Recover: Incident Recovery Plan Execution" category has six subcategories, all of which apply to routing security.

Table 21 - Recover: Incident Recovery Plan Execution (RC.RP)

Subcategory	Applicability to Internet Routing
RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process.	Applicable, no routing-specific considerations.

Subcategory	Applicability to Internet Routing
RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed.	Recovery actions related to routing incidents include adjustment of routing configuration and/or policies (e.g., route filtering, ACLs) and/or other configuration parameters For example, one workaround to allow routing to work during recovery might involve disabling RPKI ROV validation (making use of its implicit, default "fail open" design; see [RFC 7646], which describes a somewhat analogous approach in DNSSEC through the use of a "Negative Trust Anchor"). Temporary disabling can allow the routing system to continue operating while remediation is occurring.
RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration.	The integrity of routing-related backups of routing policies (e.g., route filtering, ACLs) and other configurations is verified before being used for restoration.
RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms.	Applicable, no routing specific considerations.
RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed.	The normal operating status of routing is verified, including the normal operating status of RPKI ROV, route filtering, routing sessions, routing tables, etc.
RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed.	The end of a routing incident recovery is declared, e.g., after the offending party has stopped advertising the problematic BGP updates and the problematic routes have been withdrawn and/or cleared from the routing tables. Documentation of the routing incident analysis, handling, and lesson learned is completed.

5.6.2 Recover: Incident Recovery Communication (RC.CO)

Restoration activities are coordinated with internal and external parties.

The "Recover: Incident Recovery Communication" category has two subcategories, both of which apply to routing security.

Table 22 - Recover: Incident Recovery Communication (RC.CO)

Subcategory	Applicability to Internet Routing
RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders.	Designated internal and external stakeholder (e.g., the offending AS, affected customers) are informed of the recovery activities and progress in restoring routing.
RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging.	Based on organizationally approved methods, some technical details of the routing incident may be shared with the public, e.g., the timeline of incidents, propagation path of the offending BGP updates, ending of the incidents, etc.

6 CONCLUSION

This routing security profile, aligned with NIST CSF 2.0, takes a risk management approach to internet routing. It also outlines common routing security controls and solutions—including IRRs, AS path filtering, and RPKI—for use by network and security engineers to enhance routing security, particularly BGP security. This profile is not intended to be a complete approach to cybersecurity risk management overall but rather a focal point that applies the principles of NIST's CSF to routing security. As with any endeavor in security, this profile will evolve over time with changes to the NIST CSF, routing and security technologies, and the security threat landscape.

It is our hope that this routing security profile provides a roadmap for any organization—large or small—looking to improve the routing security posture of their network environments. By helping the internet routing community increase awareness of routing security risks and how to manage those risks properly, we all contribute to the broader goal of creating a more secure and resilient global internet infrastructure.

Appendix I Acknowledgements

We wish to thank the following co-authors of this document.

Co-Author	Company Affiliation
Tao Wan	CableLabs
Taylor Harris	Charter Communications
Tony Tauber	Comcast
Antoin Verschuren	Liberty Global
Miles McCredie	Midcontinent Communications (Midco)

We wish to thank the following individuals who contributed to and/or reviewed this document.

Contributors and Reviewers	Company Affiliation
Joy Garcia	CableLabs
Gabby Gordon	CableLabs
Melanie Parker	CableLabs
Brian Scriber	CableLabs
Priya Shrinivasan	CableLabs
Rich Compton	Comcast
Mark Goodwin	Cox
Rob Cantu	NCTA
Rich Deprez	TDS Telecom

* * *