CableLabs®
Security

Cybersecurity Framework Profile for Internet Routing

CL-GL-RS-Profile-V01-240123

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-V01-240123			
Document Title:	Cybersecurity Framework Profile for Internet Routing			
Revision History:	V01 – Released 01/23/24			
Date:	January 23, 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

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. Without necessary security controls, routing protocols like the Border Gateway Protocol (BGP) are vulnerable to attack and misconfiguration, which can lead to network disruptions and service outages. Implementation of reliable and secure routing is essential for the proper functioning of communications network infrastructure.

This Routing Security Profile covers core routing protocols, including BGP, and emerging technologies, like Resource Public Key Infrastructure (RPKI). It serves as an actionable guide for network engineers, security analysts, and executives to evaluate and enhance routing security. Key topics covered with recommendations on improving BGP security include 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 INTRODUCTION

1.1 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, has three goals.

- 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.
- 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.
- 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

- 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

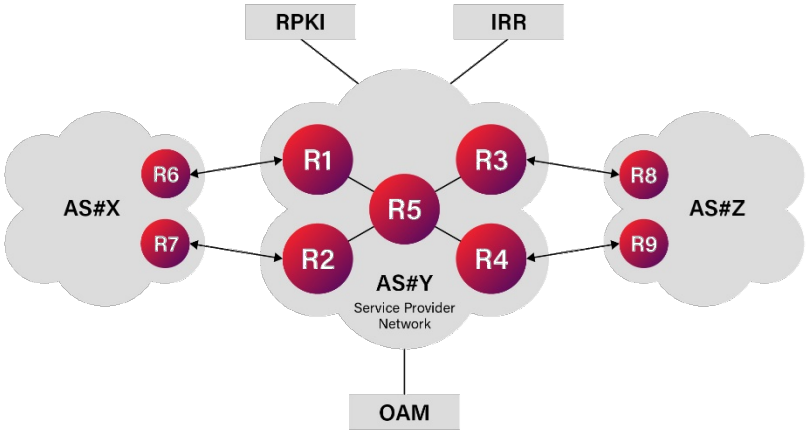

Figure 1 - Service Provider Network Routing Infrastructure

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.

[NIST CSF 1.1] NIST Cybersecurity Framework v1.1, April 2018, 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 800-53 Rev. 5] NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

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

[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.

NIST SP 800-189, "Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation," December 2019, https://csrc.nist.gov/pubs/sp/800/189/final.

2.3 Reference Acquisition

All URLs in this document are valid as of December 18, 2023.

- 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
- Internet Engineering Task Force (IETF) Secretariat, 48377 Fremont Blvd., Suite 117, Fremont, California 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
DDoS	distributed denial of service
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: Identify, Protect, Detect, Respond, and Recover [CSF 1.1].

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) 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 information between network operators. IRRs allow participants to publish details about their network routes and policies. Other operators can then query an IRR to retrieve routing data instead of relying solely on periodic exchanges via routing protocols (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.

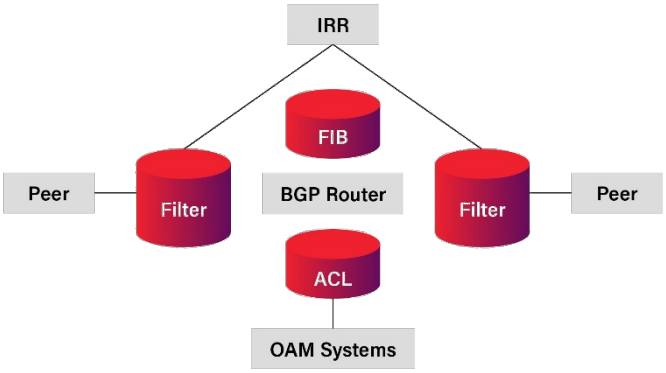

Figure 2 - IRR Used to Facilitate Routing Filtering

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. It can also involve setting filters on both ingress and egress routers to only allow routes traversing certain permissible ASNs, known as peer locking. 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 specialized framework that utilizes cryptographic certificates (Figure 3) to help provide a secure publication structure for information related to Internet routing. 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)—ROAs are digitally signed objects that authorize the routing of IP addresses by a specific AS (network organization).

Route Origin Validation (ROV)—ROV enables verification that route announcements match the ASN specified in the corresponding ROA. This prevents route hijacking and invalid route announcements by ensuring prefixes are announced only by authorized networks.

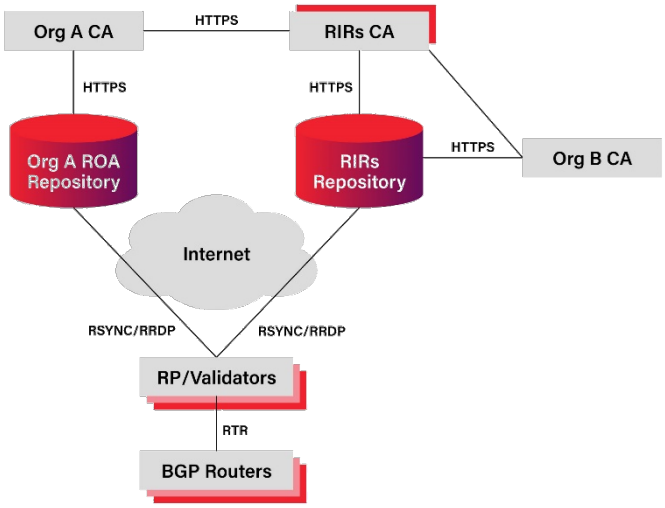

Figure 3 - RPKI Architecture

4.2 Cybersecurity Framework Overview

The NIST Cybersecurity Framework [NIST CSF 1.1] consists of three main components.

- The Framework Core provides a set of cybersecurity activities, desired outcomes, and references that are common across critical infrastructure sectors.
- The Framework Implementation Tiers provide context on how an organization views cybersecurity risk and manages the risk in a progressive manner from Tier 1 (Partial) to Tier 4 (Adaptive).
- The Framework Profiles can be considered as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario.

The Framework Core consists of four elements: functions, categories, subcategories, and informative references. At the highest level are functions: Identify, Protect, Detect, Respond, and Recover. Categories are subdivisions of a function, and subcategories further divide categories into specific outcomes.

The five functions are briefly described below.

1. Identify—Develop organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
2. Protect—Develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services.
3. Detect—Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4. Respond—Develop and implement the appropriate activities to react to a detected cybersecurity incident.
5. Recover—Develop and implement appropriate activities to maintain resilience and to restore capabilities or services that were impaired because of a cybersecurity event.

5 ROUTING SECURITY PROFILE

This Routing Security Profile section was created using the Cybersecurity Framework, 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, their applicability to routing security, and related informative references. The informative references included in the tables provide additional guidance to aid practitioners when applying this profile.

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 (including those considered not applicable) in the context of their organization and follow the recommendations as needed.**

5.1 Identify

The Identify (ID) function defines six categories.

- Asset Management (AM)
- Business Environment (BE)
- Governance (GV)
- Risk Assessment (RA)
- Risk Management Strategy (RM)
- Supply Chain Risk Management (SC)

All subcategories in each of the six categories apply to routing security.

5.1.1 Identify: Asset Management Category

Assets including data, personnel, devices, systems, and facilities and prioritization are important factors in other functions and activities, such as contingency planning for future attacks, responding to malware events, emergency responses, and recovery actions. Asset management will assist in prioritizing response and recovery activities. In the context of routing security, organizations need to inventory internal and external 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 six subcategories, all of which apply to routing security, but one of them applies with no routing-specific considerations.

Subcategory	Applicability to Internet Routing	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 certificate 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
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

Subcategory	Applicability to Internet Routing	Informative References
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

5.1.2 Identify: Business Environment Category

In the context of routing, identify the dependencies, obligations, and relationships between different organizations and their stakeholders to resolve any differences.

The "Identify: Business Environment" category has five subcategories, all of which apply to routing security, but three of them apply with no routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	Network operators should identify their role in the routing supply chain. Are they a stub network or a transit network? The impact of compromised routes to them and their partners should be understood.	[NIST SP 800-53 Rev. 5]: CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Identify the role within the nation's critical infrastructure and the sector to identify the underlying risk if the routing system is compromised.	[NIST SP 800-53 Rev. 5]: PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, CP-11, SA-13, SA-14

5.1.3 Identify: Governance Category

Document and review the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements, and inform the management of cybersecurity risk.

The "Identify: Governance" category has four subcategories, all of which apply to routing security without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
ID.GV-1: Organizational cybersecurity policy is established and communicated	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: XY-1 controls from all security control families
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: PS-7, PM-1, PM-2
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: XY-1 controls from all security control families
ID.GV-4: Governance and risk management processes address cybersecurity risks	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: SA-2, PM-3, PM-7, PM-9, PM-10, PM-11

5.1.4 Identify: Risk Assessment Category

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. 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 six subcategories, all of which apply to routing security without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
ID.RA-1: Asset vulnerabilities are identified and documented	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: SI-5, PM-15, PM-16
ID.RA-3: Threats, both internal and external, are identified and documented	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: RA-3, SI-5, PM-12, PM-16
ID.RA-4: Potential business impacts and likelihoods are identified	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: RA-2, RA-3, SA-14, PM-9, PM-11
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: RA-2, RA-3, PM-16
ID.RA-6: Risk responses are identified and prioritized	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: PM-4, PM-9

5.1.5 Identify: Risk Management Category

In the context of routing security, the risk management strategy must be informed by the tolerances and constraints of the contributing organizations. A level of collaboration and negotiation will be required across the partners to ensure a consistent and compatible set of risk management processes and procedures.

The "Identify: Risk Management" category has three subcategories, all of which apply to routing security without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: PM-9
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: PM-9
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: SA-14, PM-8, PM-9, PM-11

5.1.6 Identify: Supply Chain Risk Management Category

Supply chain risk management (SCRM) is typically an intra-organization function. In the context of routing security, organizations will need to understand the partner's SCRM so that the impacts of any risk inherited by partners is understood and within the level of the organization's tolerance.

The "Identify: Supply Chain Risk Management" category has five subcategories, all of which apply to routing without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: SA-9, SA-12, PM-9
ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: SA-9, SA-11, SA-12, PM-9
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

5.2 Protect

The objectives of the Protect function are

- to protect locally originated routing information by accurately documenting the origination of assigned address prefixes;
- to protect the routers, management infrastructure, and related operational data; and
- to ensure continuous operation of the routing system by using the documented response and recovery plans.

The Protect (PR) function defines six categories.

- Identity Management, Authentication, and Access Control (AC)
- Awareness and Training (AT)
- Data Security (DS)
- Information Protection Processes and Procedures (IP)
- Maintenance (MA)
- Protective Technology (PT)

All subcategories in each of the six categories apply to routing security.

5.2.1 Protect: Identity Management, Authentication, and Access Control Category

Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices. Routing security is uniquely challenging and important because propagation of invalid routes can impact many users and networks.

The "Protect: Identity Management, Authentications, and Access Control" category has seven subcategories, all of which apply to routing security, but five of them apply with no routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	Routing infrastructure identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes. In addition to accounts and credentials for access to the relevant systems, credentials for external relationships should also be considered. Some examples are • BGP peer authentication (TCP-AO or TCP-MD5), • access to RIR systems, and • access to systems such as peeringDB.	[NIST SP 800-53 Rev. 5]: AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 [RFC 2385], [RFC 5925]
PR.AC-2: Physical access to assets is managed and protected	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
PR.AC-3: Remote access is managed	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AC-1, AC-17, AC-19, AC-20, SC-15
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Access permissions and authorization to RIRs and IRRs and other routing assets are managed, incorporating the principles of least privilege and separation of duties.	[NIST SP 800-53 Rev. 5]: AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AC-4, AC-10, SC-7
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5.2.2 Protect: Awareness and Training Category

The Awareness and Training category is not unique to routing security. Its focus is privileged users who operate, monitor, and maintain equipment that interfaces with the organization and third-party partners. Within an ASN, third-party and partner relationships vary widely and are coordinated in advance. Third-party partner relationships to consider in the routing security context include RIR or other IRR databases, RPKI ROA creation and publication, and industry organizations such as peeringDB.

The "Protect: Awareness and Training" category has five subcategories, all of which apply to routing security, but four of them apply with no routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
PR.AT-1: All users are informed and trained	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AT-2, PM-13
PR.AT-2: Privileged users understand their roles and responsibilities	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AT-3, PM-13
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	Applicable. Third-party stakeholders such as peering partners need to follow routing security best common practice such as deploying RPKI ROAs and ROV.	[NIST SP 800-53 Rev. 5]: PS-7, SA-9, SA-16 [RFC 6482], [RFC 6811]
PR.AT-4: Senior executives understand their roles and responsibilities	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AT-3, PM-13
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AT-3, IR-2, PM-13

5.2.3 Protect: Data Security Category

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

The "Protect: Data Security" category has eight subcategories, all of which apply to routing security, but one of them applies with no routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
PR.DS-1: Data-at-rest are protected	Prefixes and AS pairs, indicating which AS is authorized to announce one or a set of prefixes owned or managed by the organization, are digitally signed by ROAs. Configuration data (such as filtering lists) are managed properly.	[NIST SP 800-53 Rev. 5]: MP-8, SC-12, SC-28 [RFC 6482] [RPKI-BCP], CableLabs RPKI Deployment BCP [RFC 7115], [RFC 9319]
PR.DS-2: Data-in-transit are protected	Routing data (e.g., routing updates) in transit are protected and validated, e.g., by using ROV.	[NIST SP 800-53 Rev. 5]: SC-8, SC-11, SC-12 [RFC 6811]
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Applicable. Particularly, IP prefix transfer needs to be reflected in ROAs.	[NIST SP 800-53 Rev. 5]: CM-8, MP-6, PE-16
PR.DS-4: Adequate capacity to ensure availability is maintained	Adequate capacity of routing infrastructure (routing tables, ACLs, ports, links, router CPU, etc.) is maintained to ensure availability.	[NIST SP 800-53 Rev. 5]: AU-4, CP-2, SC-5
PR.DS-5: Protections against data leaks are implemented	Protections against routing data leaks (e.g., route leaks and other data) are implemented, e.g., via ROV, BGP Role, and filtering.	[NIST SP 800-53 Rev. 5]: AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 [RFC 6811], [RFC 9234]
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Applicable. Particularly, ROAs need to be validated by a relying party.	[NIST SP 800-53 Rev. 5]: SC-16, SI-7 [RFC 6488]
PR.DS-7: The development and testing environment(s) are separate from the production environment	Applicable. For example, new RPKI deployment, new BGP attributes, and new filtering policies need to be tested before deployed in production environment.	[NIST SP 800-53 Rev. 5]: CM-2
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: SA-10, SI-7

5.2.4 Protect: Information Protection Processes and Procedures Category

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to protect information systems and assets. In the context of routing security, policies must be coordinated among external partners and stakeholders in addition to internal entities.

The "Protect: Information Protection Processes and Procedures" category has twelve subcategories, all of which apply to routing security, but eight of them apply with no routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	Applicable, particularly following ROA, ROV, and filtering best common practices.	[NIST SP 800-53 Rev. 5]: CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 [RPKI-BCP], CableLabs RPKI Deployment BCP [RFC 7115], [RFC 9319]
PR.IP-2: A System Development Life Cycle to manage systems is implemented	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17

Subcategory	Applicability to Internet Routing	Informative References
PR.IP-3: Configuration change control processes are in place	Applicable. Particularly, the processes of managing network topology changes, prefix announcement changes, network policy changes, and peering relationship changes are in place, among other changes.	[NIST SP 800-53 Rev. 5]: CM-3, CM-4, SA-10
PR.IP-4: Backups of information are conducted, maintained, and tested	Applicable. Backups of routing infrastructure information (e.g., routes, configurations, policies) are conducted, maintained, and tested.	[NIST SP 800-53 Rev. 5]: CP-4, CP-6, CP-9
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
PR.IP-6: Data are destroyed according to policy	Routing infrastructure data (e.g., prefix announcements, ROAs) are destroyed according to policy.	[NIST SP 800-53 Rev. 5]: MP-6
PR.IP-7: Protection processes are improved	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
PR.IP-8: Effectiveness of protection technologies is shared	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AC-21, CA-7, SI-4
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
PR.IP-10: Response and recovery plans are tested	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-4, IR-3, PM-14
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
PR.IP-12: A vulnerability management plan is developed and implemented	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: RA-3, RA-5, SI-2

5.2.5 Protect: Maintenance Category

Maintenance and repairs of routing infrastructure and associated information stores are performed consistent with policies and procedures. The policies and procedures that pertain to maintenance and repairs within the routing environment should be agreed upon in advance before connecting to the global Internet and should be reviewed periodically.

The "Protect: Maintenance" category has two subcategories that apply to routing security without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: MA-2, MA-3, MA-5, MA-6
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: MA-4

5.2.6 Protect: Protective Technology Category

Routing, particularly in the global Internet, requires collaboration and cooperation. Organizations should consider using protective technologies with standardized interfaces, formats, and protocols to facilitate collaboration and ensure compatibility.

The "Protect: Protective Technology" category has five subcategories, all of which apply to routing security, but three of them apply with no routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AU Family
PR.PT-2: Removable media is protected, and its use restricted according to policy	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AC-3, CM-7
PR.PT-4: Communications and control networks are protected	The routing infrastructure's in-band and out-of-band communications are protected. eBGP sessions can be protected with GTSM, TCP-MD5 or TCP-AO, and filtering (see [RFC 7454], BGP OpsSec). Control sessions from management stations to BGP routers need to be protected, e.g., by using SSH or TLS.	[NIST SP 800-53 Rev. 5]: AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43 [RFC 7454] (BGP OpsSec) [RFC 5082] (GTSM) [RFC 2385] (TCP-MD5) [RFC 5925] (TCP-AO) [RFC 4253] (SSH) [RFC 8446] (TLS1.3)
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Applicable. Particularly, if a delegated RPKI model is used, loading balancing and anti-DDoS protections need to be considered.	[NIST SP 800-53 Rev. 5]: CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

5.3 Detect

The Detect function requires the establishment of a baseline for network behavior, which forms the basis for the development and deployment of appropriate activities to monitor for anomalous events and notify users and applications upon their occurrence. The Detect function is informed by the Identify function and is enabled by the Protect function.

The Detect (DE) function defines three categories.

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

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.

5.3.1 Detect: Anomalies and Event Category

The "Detect: Anomalies and Event" category has five subcategories, all of which apply to routing security, but four of them apply with no routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	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.	[NIST SP 800-53 Rev. 5]: AC-4, CA-3, CM-2, SI-4

Subcategory	Applicability to Internet Routing	Informative References
DE.AE-2: Detected events are analyzed to understand attack targets and methods	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AU-6, CA-7, IR-4, SI-4
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
DE.AE-4: Impact of events is determined	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, IR-4, RA-3, SI-4
DE.AE-5: Incident alert thresholds are established	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: IR-4, IR-5, IR-8

5.3.2 Detect: Security Continuous Monitoring Category

Routing networks and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. In addition, external networks (e.g., global routing) can also be monitored to identify events that may have potential impact on the operator's network.

The "Detect: Security Continuous Monitoring" category has eight subcategories, six of which apply to routing security without routing-specific considerations; one applies with a routing-specific consideration, and one does not apply.

Subcategory	Applicability to Internet Routing	Informative References
DE.CM-1: The network is monitored to detect potential cybersecurity events	Routing networks and assets including external networks such as global routing are monitored continuously.	[NIST SP 800-53 Rev. 5]: AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CA-7, PE-3, PE-6, PE-20
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
DE.CM-4: Malicious code is detected	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: SI-3, SI-8
***DE.CM-5:** Unauthorized mobile code is detected*	*Not applicable.*	*[NIST SP 800-53 Rev. 5]: SC-18, SI-4, SC-44*
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CA-7, PS-7, SA-4, SA-9, SI-4
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
DE.CM-8: Vulnerability scans are performed	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: RA-5

5.3.3 Detect: Detection Processes Category

The "Detect: Detection Processes" category has five subcategories, all of which apply to routing security without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CA-2, CA-7, PM-14
DE.DP-2: Detection activities comply with all applicable requirements	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
DE.DP-3: Detection processes are tested	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
DE.DP-4: Event detection information is communicated	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AU-6, CA-2, CA-7, RA-5, SI-4

Subcategory	Applicability to Internet Routing	Informative References
DE.DP-5: Detection processes are continuously improved	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

5.4 Respond

The activities in the Respond function support the ability to contain the impact of an incident by developing and implementing appropriate responses to a detected cybersecurity attack or anomalous incident. The Respond function actions are triggered by the outputs generated by the Detect function. The Protect function enables the Respond function to execute the proper response to an event according to a predefined plan.

The Respond (RS) function defines five categories.

- Response Planning (RP)
- Communications (CO)
- Analysis (AN)
- Mitigation (MI)
- Improvements (IM)

All subcategories in each of the five categories apply to routing security.

5.4.1 Respond: Response Planning Category

The response plan needs to be developed in advance to ensure that all participants are aware of their obligations and responsibilities during and after an incident.

The "Respond: Response Planning" category has one subcategory that applies to routing security without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
RS.RP-1: Response plan is executed during or after an incident	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, CP-10, IR-4, IR-8

5.4.2 Respond: Communications Category

The Respond function activities are coordinated with internal and external stakeholders (e.g., with external BGP peers).

The "Respond: Communications" category has five subcategories, all of which apply to routing security without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
RS.CO-1: Personnel know their roles and order of operations when a response is needed	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, CP-3, IR-3, IR-8
RS.CO-2: Incidents are reported consistent with established criteria	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AU-6, IR-6, IR-8
RS.CO-3: Information is shared consistent with response plans	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, IR-4, IR-8
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: SI-5, PM-15

5.4.3 Respond: Analysis Category

Analysis is conducted to ensure effective response and support recovery activities.

The "Respond: Analysis" category has five subcategories, all of which apply to routing security without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
RS.AN-1: Notifications from detection systems are investigated	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
RS.AN-2: The impact of the incident is understood	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, IR-4
RS.AN-3: Forensics are performed	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: AU-7, IR-4
RS.AN-4: Incidents are categorized consistent with response plans	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, IR-4, IR-5, IR-8
RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers)	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: SI-5, PM-15

5.4.4 Respond: Mitigation Category

Activities are performed to prevent the expansion of an event, mitigate its effects, and resolve the incident.

The "Respond: Mitigation" category has three subcategories, all of which apply to routing security, but one of them applies with no routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
RS.MI-1: Incidents are contained	ROA, ROV, and filtering are deployed. Contact offending ASN and their upstream providers. Review policy in place and adjust accordingly. Seek expert assistance if needed.	[NIST SP 800-53 Rev. 5]: IR-4
RS.MI-2: Incidents are mitigated	ROA, ROV, and filtering are deployed. Contact offending ASN and their upstream providers. Review policy in place and adjust accordingly. Seek expert assistance if needed.	[NIST SP 800-53 Rev. 5]: IR-4
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CA-7, RA-3, RA-5

5.4.5 Respond: Improvements Category

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

The "Respond: Improvements" category has two subcategories, both of which apply to routing security without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
RS.IM-1: Response plans incorporate lessons learned	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, IR-4, IR-8
RS.IM-2: Response strategies are updated	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, IR-4, IR-8

5.5 Recover

The Recover function develops and implements the appropriate activities to maintain resilience and restore any capabilities or services that were impaired because of a cybersecurity event.

The Recover (RC) function defines three categories.

- Recovery Planning (RP)
- Improvements (IM)
- Communication (CO)

All three categories and their subcategories apply to routing security but without any routing-specific considerations.

5.5.1 Recover: Recovery Planning Category

Recovery processes and procedures are executed and maintained to ensure the restoration of systems or assets affected by cybersecurity incidents.

The "Recover: Recovery Planning" category has one subcategory that applies to routing security without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-10, IR-4, IR-8

5.5.2 Recover: Improvements Category

Recovery planning and processes are improved by incorporating lessons learned into future activities.

The "Recover: Improvements" category has two subcategories, both of which apply to routing security without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
RC.IM-1: Recovery plans incorporate lessons learned	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, IR-4, IR-8
RC.IM-2: Recovery strategies are updated	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, IR-4, IR-8

5.5.3 Recover: Communications Category

Public relationships are managed properly, and recovery activities are coordinated with internal and external parties.

The "Recover: Communications" category has three subcategories, all of which apply to routing security without routing-specific considerations.

Subcategory	Applicability to Internet Routing	Informative References
RC.CO-1: Public relations are managed	Applicable, no routing-specific considerations.	
RC.CO-2: Reputation is repaired after an incident	Applicable, no routing-specific considerations.	
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	Applicable, no routing-specific considerations.	[NIST SP 800-53 Rev. 5]: CP-2, IR-4

6 CONCLUSION

This Routing Security Profile 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 can help the Internet routing community increase awareness of routing security risks and manage those risks properly, leading to further improvement of the routing security of a particular network as well as global routing security overall.

Appendix I Acknowledgements

We wish to thank the following co-authors (in alphabetical order) of this document.

Co-authors	Company Affiliation
Jody Beck	Charter Communications
Rich Compton	Charter Communications
Miles McCredie	Midcontinent Communications (Midco)
Tony Tauber	Comcast
Tao Wan	CableLabs

We wish to thank the following individuals (in alphabetical order) who contributed to and/or reviewed this document.

Contributors and Reviewers	Company Affiliation
Steve Goeringer	CableLabs
Steve Mace	NCTA
Melanie Parker	CableLabs
Priya Shrinivasan	CableLabs
Rikin Thakker	NCTA
Matt Tooley	Charter Communications

* * *