Canadian Radio-television and Telecommunications Commission
Conseil de la radiodiffusion et des télécommunications canadiennes

Compliance and Enforcement and Telecom Decision CRTC 2025-142

PDF version

Gatineau, 13 June 2025

Public record: 1011-NOC2021-0009

Development of a framework to limit botnet traffic

Summary

The Commission helps ensure that Canadians have access to safe and reliable telecommunications services through its work under the *Telecommunications Act* (the Act) and Canada's Anti-Spam Legislation (CASL). Under the Act, the Commission plays a narrow role by regulating telecommunications service providers (TSPs). Under CASL, the Commission helps protect Canadians from online spam along with the Competition Bureau and the Office of the Privacy Commissioner, by promoting and monitoring compliance within a civil regulatory regime.

Botnets are networks of computers, cellphones, or other devices that have been infected with malware. This allows individuals or groups to control the devices without the knowledge or consent of their owners. Botnets can be used for sending spam to Canadians or for other harmful activities. In Compliance and Enforcement and Telecom Decision 2022-170, the Commission found that regulatory action is necessary so that TSPs can help disrupt botnets and protect Canadians from the harm they cause. The Commission outlined the guiding principles for a regulatory framework to block harmful botnet activities in that decision.

The Commission asked the CRTC Interconnection Steering Committee (CISC) Network Working Group (NTWG) to provide a report on which harmful activities should be blocked by the framework, and on potential blocking methods. The NTWG is composed of expert technical groups that include TSPs, federal departments with public safety mandates, and other industry experts.

Based on the record of this proceeding and the CISC NTWG's report, the Commission is establishing a framework that sets out the terms and conditions to allow Canadian carriers to block botnets and other harmful activities within their networks before reaching Canadians' devices. This blocking must be done in accordance with the blocking framework set out in the appendix to this decision, starting on **12 August 2025**.

In Compliance and Enforcement and Telecom Notice of Consultation 2025-143, also published today, the Commission is gathering views on whether the framework should be expanded to include other blocking methods.

Canada

Background

1. In Compliance and Enforcement and Telecom Decision 2022-170 (the Decision), the Commission found that regulatory action is necessary to address harmful botnet traffic.[1] The Commission determined that the most appropriate regulatory approach is to create a framework that establishes the minimum standards for Canadian carriers to receive the Commission's approval to block botnet traffic at the network level.

2. In the Decision, the Commission also determined that the framework would be guided by the principles of necessity, customer privacy, accountability, transparency, and accuracy. The Commission asked the CRTC Interconnection Steering Committee (CISC) to examine several issues to help develop minimum standards that are consistent with these guiding principles.

3. On 31 May 2023, the CISC Network Working Group filed a report entitled *Development of a network-level blocking framework to limit botnet traffic and strengthen Canadians' online safety* (NTRE080) [the Report], which made recommendations on the types of activities to be blocked by the framework, how blocklists should be used by carriers, and whether additional blocking methods should be included under the framework.

4. Contributors to the Report included telecommunications service providers (TSPs), Bell Canada, Rogers Communications Canada Inc. (Rogers), Saskatchewan Telecommunications, Shaw Communications Inc. (Shaw), TekSavvy Solutions Inc., and TELUS Communications Inc. (TELUS), as well as the Canadian Centre for Cybersecurity (CCCS) of the Communications Security Establishment, the Canadian Internet Registration Authority (CIRA), the Competitive Network Operators of Canada and the Independent Telecommunications Providers Association (ITPA), and the National Cybercrime Coordination Unit (NC3) of the Royal Canadian Mounted Police.

5. The Commission received comments on the Report from Bell Canada, the CCCS, the ITPA, the Public Interest Advocacy Centre (PIAC), Rogers, NC3, TELUS, and one individual.

6. In this decision, the Commission establishes a framework authorizing Canadian carriers to block botnets at the network level using authorized blocklists. The framework sets out the minimum standards for Canadian carriers to receive the Commission's approval to engage in network-level blocking, pursuant to section 36 of the *Telecommunications Act* (the Act). This section of the Act states that Canadian

---

[1] A botnet is a network of malware-infected devices, known as bots, controlled without the knowledge and consent of the device owners, and used for malicious purposes. Botnet traffic is the Internet traffic that flows between bots and their points of control, known as command-and-control servers.

carriers need the Commission's approval to control or influence the content of telecommunications.

Issues

7. Based on the Report and the comments received on the Report, the Commission has identified the following issues to be addressed:

    - What should the scope of the framework be?
    - How should blocklists be implemented?
    - Which blocking methods should the framework authorize?
    - What other aspects of the framework should be considered?

What should the scope of the framework be?

Definitions

8. In the Report, CISC noted that most contributors agreed with the definitions of cyber security and cyber attack proposed in the Decision.

Commission's analysis

9. In light of this broad consensus, the following definitions will be used for the purposes of the framework:

    Cyber security: A body of technologies, processes, practices, and response and mitigation measures designed to protect against cyber attacks in order to ensure confidentiality, integrity, and availability of electronic information.

    Cyber attack: Malicious use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.

10. The Commission notes that the term "cyber security" in this context applies to the security of Internet services that carriers provide to consumers. The term does not apply to carriers' use of Internet traffic management practices (ITMPs) to manage congestion on their networks and protect their integrity (see Telecom Regulatory Policy 2009-657).

Definition of indicator of compromise

11. Contributors to the Report were unable to agree on a single definition of indicator of compromise (IOC) to recommend to the Commission. Some contributors disagreed with the definition proposed in the Decision based on the argument that an IOC is made up of multiple data points rather than one. Others noted that they could not properly assess the accuracy of the Commission's proposed definition without knowing more about how IOCs will be used in the context of the framework.

Positions of parties

12. Since an IOC consists of data, Bell Canada and Rogers suggested removing the word "forensic" from the definition. Bell Canada also argued that an IOC should not be defined as a combination or series of data points because maintaining IOCs based on multiple data points within a botnet blocklist is difficult.

Commission's analysis

13. The Commission is of the view that, in the context of the framework, IOC simply refers to identifiers to be blocked for cyber security purposes. Identifiers can include one or more pieces of data, including, for example, a domain name and an Internet Protocol (IP) address and port number.

14. The Commission agrees that there is no need to include the term "forensic" in the definition of IOC. It also considers that the last two sentences of the proposed definition are unnecessary, because they refer to how IOCs are generally used by the cyber security community.

15. Therefore, the initial definition of IOC will be revised to the following:

> An IOC is an identifier used by carriers to block network traffic for cyber security purposes that indicates, with a high degree of confidence, intrusion on a system and that malicious activity is occurring. In other words, an IOC is a technical characteristic of a particular cyber attack. In the context of a blocklist, an IOC may consist of, for example (i) a domain name, or (ii) an IP address and port number.

Applying the framework to the blocking of all IOCs

16. In the Report, CISC noted that most contributors recommended that the framework apply only to botnet-specific blocking, because that was the original scope proposed by the Commission.

17. However, CIRA and NC3 noted that from a technical point of view, the framework could apply to the blocking of all IOCs and not just botnet traffic. They argued that any blocking that respects the guiding principles of the framework and is done for cyber security purposes should be allowed.

Positions of parties

18. Bell Canada recommended that the framework focus on preventing botnet traffic, and PIAC proposed limiting blocking to botnet traffic to minimize the risk of blocking non-malicious traffic.

19. Bell Canada, Shaw, and TELUS raised technical concerns about the types and volume of IOCs to be blocked. They noted that using blocklists that include IOCs for non-botnet cyber threats would require a large processing capacity, which could harm network performance.

20. However, the CCCS and NC3 pointed out that blocking only botnet traffic would address only part of the damage caused by malicious traffic, and that identifying only IOCs linked to botnet traffic within threat feeds would be difficult. Therefore, they suggested including blocking malicious non-botnet traffic in the framework.

Commission's analysis

21. In the Decision, the Commission stated that botnets, malware, and computer intrusions are intertwined, making it impractical and inefficient to block only botnet traffic and not block other types of IOCs. The Commission also noted that it may not be practical to isolate botnet traffic identified through specific IOCs, because the IOCs used for the purpose of blocking traffic do not specifically identify botnets. Instead, the IOCs identify more generally malware traffic or traffic suggestive of computer intrusions.

22. In the Decision, the Commission also noted that the policy justification for blocking botnet traffic (i.e., the harm caused to Canadians) applies equally to traffic identified by other IOCs.

23. Regarding the concern that the use of large blocklists could harm network performance, the Commission notes that the framework does not require the use of a specific blocklist or impose a minimum blocking threshold. Carriers that opt into the framework can control the types and volume of IOCs that they block so long as they abide by its terms and conditions.

24. The Commission considers that a framework that focuses on all IOCs rather than just those that only identify botnet traffic would maximize its effectiveness in protecting Canadians, be technically feasible, and be appropriate as a matter of policy.

25. The Commission therefore determines that the scope of the framework will extend to the blocking of all IOCs.

How should blocklists be implemented?

Centralized blocklist

26. In the Decision, the Commission asked CISC whether there is an independent expert body that can maintain a centralized blocklist for use by TSPs, and how this expert body would handle false-positive complaints when non-malicious traffic is incorrectly blocked. It also asked whether TSPs and other stakeholders can request the addition or removal of specific IOCs from the blocklist.

27. While CISC was unable to identify an independent expert body to maintain a centralized blocklist, it recommended that if an expert body is identified to handle false-positive complaints, it should be responsible for processing these complaints and updating the blocklist.

Positions of parties

28. Bell Canada and Rogers suggested that, given its experience and expertise in cyber security, the CCCS should manage a centralized blocklist. TELUS, on the other hand, proposed that Canadian TSPs manage a centralized blocklist.

29. The CCCS stated that it cannot maintain a centralized blocklist because this regulatory function is inconsistent with its mandate.

Commission's analysis

30. Since no independent expert body able to manage a centralized blocklist was identified, the Commission will not decide on this issue at this time.

Third-party blocklists

31. In the Decision, the Commission asked CISC how third-party blocklists should be accredited if they are included in the framework and how the public should submit false-positive complaints to ensure third-party blocklists are updated.

32. In the Report, CISC could not identify an organization able to manage the accreditation of third-party blocklists. However, it suggested that a central body within government or the telecommunications industry could perform this function.

33. CISC added that accrediting multiple blocklists would, among other things, give TSPs the flexibility to choose a blocklist that fits their preferences. It also recommended that the owners of third-party blocklists be responsible for handling false-positive complaints and updating their blocklists as needed.

Positions of parties

34. Bell Canada, Rogers, and TELUS agreed on the need for a centralized accreditation process to ensure third-party blocklists meet minimum criteria. Bell Canada recommended that the CCCS manage this process and proposed accreditation criteria for blocklist providers.

35. The CCCS recommended that a central committee manage the accreditation process. It indicated that it would contribute its experience in cyber security to the committee, but that it should not have any power to make decisions.

36. The ITPA submitted that a centralized accreditation process is not necessary and recommended that TSPs be allowed to use any third-party blocklist that meets pre-established criteria. The ITPA suggested that TSPs submit the blocklists they are using to an entity like the Commission, which could publish a register of blocklists used by Canadian TSPs.

37. TELUS indicated that carriers may need to use multiple blocklists since there is limited overlap between them.

38. Regarding false-positive complaints, Bell Canada and the ITPA suggested that a centralized web portal be created to allow Canadians to check and report false positives. However, Rogers warned that malicious actors could use this portal to identify IP addresses.

39. PIAC argued that submitting false-positive complaints should be easy for the average person and that fast responses to these complaints are crucial.

Commission's analysis

40. The Commission considers that carriers should be responsible for ensuring that the blocklists they use meet minimum criteria, since no organization was identified to manage a centralized accreditation process. The minimum criteria for blocklists are set out in sections 3.0 and 4.0 of the framework outlined in the appendix to this decision.

41. As for false-positive complaints, the Commission agrees that these should be addressed in a timely manner. Therefore, section 5.0 of the framework will require carriers to resolve complaints about a potential false positive within two business days of its receipt.

In-house blocklists

42. In the Report, CISC noted that most TSPs do not have the capacity to create and maintain their own blocklists.

Commission's analysis

43. One of the advantages of in-house blocklists is that they can enable carriers to block IOCs that are not on third-party blocklists, particularly IOCs that are specific to Canada.

44. Considering that some carriers are already using in-house blocklists and that others may be able to build their own, the Commission will allow the use of in-house blocklists under the framework, subject to the terms and conditions set out in section 4.0.

Which blocking methods should the framework authorize?

Types of blocking

45. In the Report, CISC recommended that the framework be limited to IP-based blocking because it is the most common capability supported by TSPs.

Positions of parties

46. Bell Canada and TELUS agreed that the framework should be limited to IP-based blocking. However, the CCCS and NC3 argued that such a limitation would restrict

the ability of carriers to adapt and therefore recommended that other types of blocking be authorized.

Commission's analysis

47. The purpose of a broad, technologically neutral framework is to allow carriers to implement network-level blocking to the best of their technical capabilities. Limiting the framework to IP-based blocking would not provide individual carriers with the flexibility to block to the highest of their technical capability and would constrain their ability to adapt.

48. Therefore, the Commission determines that the framework will not be limited to IP-based blocking.

Blocking methods other than blocklists

49. In the Decision, the Commission recognized that each blocking method has its own advantages and disadvantages, and that carriers may want to use multiple methods to achieve the best results. Accordingly, the Commission asked CISC whether there are any technical issues it should consider before authorizing other blocking methods under the framework.

50. CISC submitted that for blocking to be effective, carriers must use several different methods at the same time. Therefore, it recommended that carriers be given the flexibility to choose among different blocking methods.

Positions of parties

51. Rogers stated that since TSPs already use various techniques to protect customers from malicious online activity, they should have the flexibility to implement other measures alongside the blocking methods authorized under the framework.

52. An individual intervener noted that the record of this proceeding does not address port blocking, signature-based blocking or blocking based on behavioural characteristics, and blocking based on stateful packet inspection.

Commission's analysis

53. The record of the proceeding that led to the Decision showed that many carriers have been using blocking methods that are based on detecting unusual or malicious patterns in network traffic.

54. The Commission considers that all blocking methods should be authorized under the framework to ensure that they comply with the framework's minimum criteria.

55. However, the Commission currently has limited information about blocking methods other than blocklists. Therefore, in Compliance and Enforcement and Telecom Notice of Consultation 2025-143, the Commission will examine whether and how blocking methods other than blocklists should be incorporated into the framework.

What other aspects of the framework should be considered?

Choice for customers to opt in or out

56. In the Decision, the Commission asked CISC whether there is a technical need to allow individual customers to opt in or out of blocking.

57. In the Report, CISC stated that there is no technical need or indeed any way to allow customers to opt in or out of network-level blocking.

Positions of parties

58. While the individual intervener supported an opt-out option for customers, Bell Canada and TELUS agreed with CISC that it is not possible for most carriers to allow their customers to opt out of blocking, because carriers are typically not able to recognize individual users' traffic at the network level.

59. Bell Canada and Rogers also noted that including an opt-out option would reduce the effectiveness of the framework by increasing the likelihood that the devices of those who opt out will get infected and spread botnets and malware to other Canadians.

Commission's analysis

60. In the Decision, the Commission took the view that blocking should be done by default, without giving customers the option to opt in or out. The Decision noted that opt-in approaches have low uptakes and that both opt-in and opt-out approaches undermine network security and significantly increase the implementation burden and costs borne by carriers.

61. The Commission considers that allowing customers to opt in or out of network-level blocking provided by carriers is not technically feasible and would undermine the purpose of the framework. A blocking-by-default approach would ensure that all of a carrier's customers benefit from the blocking in the most efficient and effective manner. As noted in the Decision, this approach is consistent with other prominent Internet traffic blocking approaches, including the Cleanfeed blocking model and CIRA's blocking model.

62. The Commission therefore determines that blocking under the framework will be applied by default.

How to maximize the effectiveness of the framework

63. In the Decision, the Commission asked CISC what other technical elements would help maximize the uptake and effectiveness of the framework.

64. In the Report, CISC suggested that the data format for IOC blocking should be consistent to ensure compatibility across platforms, that TSPs should adopt mechanisms for intelligence sharing, and that IOCs should have expiry dates.

Commission's analysis

65. Regarding expiry dates for IOCs, the Commission considers that a mix of manual review and automated IOC delisting would help minimize false positives and ensure blocklists are accurate and up to date.

66. Regarding intelligence sharing, the Commission believes that IOC sharing among carriers would help maximize the effectiveness of the framework. However, intelligence sharing may be problematic due to the terms of use of commercial blocklists that may not allow open sharing of IOCs, as well as the possible resistance of carriers to sharing the IOCs from blocklists they have developed internally. Therefore, the Commission will only encourage carriers to share IOCs in the interest of helping one another.

67. As for requiring a consistent data format, this suggestion goes against the idea that the framework should be technologically neutral and may directly affect other parties that are not regulated by the Commission, including blocklist providers. Therefore, the Commission will let the industry and blocklist providers agree on data format standards.

Disclosure to the public

68. In the Report, CISC proposed that the ITMP disclosure requirements set out in Telecom Regulatory Policy 2009-657 be used as a model for notifying customers about the framework. It added that the framework should clearly outline what information regarding transparency is needed for Canadians to be able to make informed decisions about the carriers they want to use.

Positions of parties

69. TELUS stated that disclosure of all blocked IOCs to the public could make cyber security programs less effective, while Bell Canada recommended that the framework be made public, but not the actual IOCs.

70. PIAC emphasized that the disclosure of relevant details in plain language is very important for consumers.

71. The Commission also received comments on the need for transparency about what is being blocked and how.

Commission's analysis

72. The Commission considers that information about blocking under the framework should be made available to allow consumers to make informed decisions regarding their Internet services. To ensure transparency, this information should be in plain language and include details about the type and scope of blocking that is in place, and when and how it will be applied.

73. The Commission agrees that the list of IOCs blocked by a carrier should not be made public, since that would provide malicious actors with information they could exploit.

74. Therefore, section 6.0 of the framework will require carriers to disclose, clearly and prominently on their websites, certain information related to their blocking. These disclosure requirements are broadly consistent with the Commission's existing requirements for ITMPs.

Reporting requirements

75. The Report suggested that each TSP should provide to the Commission the number of IOCs blocked and the number of false positives reported.

Positions of parties

76. Bell Canada suggested that instead of having carriers continuously report metrics to the Commission, it would be more effective to set up comprehensive accreditation criteria and have an independent third party accredit blocklist providers.

Commission's analysis

77. Carriers' current botnet blocking practices are unclear even after a public consultation and the publication of the Report. Canadians know little about what carriers are doing in terms of cyber security blocking. Implementing reporting requirements would help the Commission monitor and evaluate the framework's performance and determine whether it is working efficiently and accomplishing its purpose.

78. The Commission considers it is in the public interest for Canadians to be aware of carriers' network-level blocking performance because network safety is part of the Internet service they pay for. In addition, more transparency may drive competition and innovation among carriers by allowing the public to identify how well carriers are performing and to make more informed decisions.

79. The Commission is, however, of the view that the reporting requirements should not be limited to the two metrics proposed by CISC. It considers that, for the purpose of evaluating the effectiveness of the framework, it would be appropriate to require more detailed information regarding carriers' blocking performance.

80. Therefore, section 7.0 of the framework will require carriers to submit some information annually about their cyber security blocking to the Commission. This includes details on the blocklists used, the number and types of unique IOCs blocked, the number and types of blocking events, and the number of false-positive or over-blocking complaints from customers. However, to reduce the immediate administrative burden associated with implementing the framework, these reporting requirements will only take effect after the public consultation initiated by

Compliance and Enforcement and Telecom Notice of Consultation 2025-143 is completed.

Privacy

81. In the Report, CISC noted that assessing traffic at the network level does not require subscriber information and therefore does not involve processing any personal information data.

Positions of parties

82. PIAC raised concerns over the possibility that certain methods of identifying and blocking botnets could involve collecting and exposing consumers' personal information.

83. Bell Canada and TELUS submitted that there is no need for more privacy safeguards because network-level botnet blocking does not involve looking at the content of messages or websites.

84. TELUS noted that since network-level security actions target malicious activity based on domain names, IP addresses, universal resource locators, unusual traffic patterns, and other network parameters, network-level blocking applies to all of a TSP's customers, not just specific ones.

Commission's analysis

85. As noted in the Decision, network-level botnet blocking usually does not involve identifying specific customers. If a carrier collects or exposes personal information to protect against cyber attacks, it must follow existing legal and regulatory obligations, including those set out in the *Personal Information Protection and Electronic Documents Act* and in various Commission decisions such as Telecom Decision 2003-33 and Telecom Regulatory Policies 2009-723 and 2017-11.

86. Considering the above, paragraph 8.2 of the framework will explicitly state that if a carrier collects, uses, or discloses personal information for activities under the framework, it must comply with all applicable laws and regulations. It will also make it clear that the framework does not permit any additional collection, use, or disclosure of personal information.

Conclusion

87. The Commission approves, in accordance with section 36 of the Act, the framework set out in the appendix to this decision. It will take effect on **12 August 2025**.

88. Under section 36 of the Act, Canadian carriers need the Commission's approval to control or influence the content of telecommunications. By blocking botnet traffic and other harmful activities, Canadian carriers may prevent the delivery of telecommunications to users, thus controlling the content of the telecommunications

they carry for the public. Accordingly, such activity falls within the scope of section 36 of the Act.

89. The framework sets out the terms and conditions that allow Canadian carriers to block botnet traffic. For now, the framework is limited to the use of third-party and in-house blocklists. However, in Compliance and Enforcement and Telecom Notice of Consultation 2025-143, the Commission will examine whether and how blocking methods other than blocklists should be incorporated into the framework.

2023 Policy Direction

90. The Commission considers that the framework will advance the telecommunications policy objectives set out in the Act[2] as well as the consumer interests and innovation objectives of the 2023 Policy Direction[3] by helping protect Canadians from botnets and making telecommunications services more reliable. The framework is designed to be technologically neutral and flexible to encourage innovation by carriers in addressing online harms, and to help protect the privacy of persons by prohibiting unauthorized access to and collection of their personal information.

Secretary General

Related documents

- *Call for comments – Proposed modifications to the framework to limit botnet traffic*, Compliance and Enforcement and Telecom Notice of Consultation 2025-143, 13 June 2025

- *Development of a network-level blocking framework to limit botnet traffic and strengthen Canadians' online safety*, Compliance and Enforcement and Telecom Decision CRTC 2022-170, 23 June 2022, as amended by Compliance and Enforcement and Telecom Decision CRTC 2022-170-1, 11 October 2022

- *Application of regulatory obligations directly to non-carriers offering and providing telecommunications services*, Telecom Regulatory Policy CRTC 2017-11, 17 January 2017

- *Regulatory measures associated with confidentiality provisions and privacy measures*, Telecom Regulatory Policy CRTC 2009-723, 25 November 2009

---

[2] The relevant objectives are: 7(b) to render reliable and affordable telecommunications services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada, (g) to stimulate research and development in Canada in the field of telecommunications and to encourage innovation in the provision of telecommunications services, (h) to respond to the economic and social requirements of users of telecommunications services, and (i) to contribute to the protection of the privacy of persons.

[3] *Order Issuing a Direction to the CRTC on a Renewed Approach to Telecommunications Policy*, SOR/2023-23, 10 February 2023.

- *Review of the Internet traffic management practices of Internet service providers*, Telecom Regulatory Policy CRTC 2009-657, 21 October 2009

- *Confidentiality provisions of Canadian carriers*, Telecom Decision CRTC 2003-33, 30 May 2003, as amended by Telecom Decision CRTC 2003-33-1, 11 July 2003

Appendix to Compliance and Enforcement and Telecom Decision CRTC 2025-142

Framework to limit botnet traffic

Definitions

Blocklist: A list of indicators of compromise (IOCs) that may be used by a carrier to block malicious Internet traffic traversing their network.

Blocklist provider: A person who owns and manages a blocklist. This person may be a carrier (for an in-house blocklist) or any other person, such as a blocklist vendor (for a third-party blocklist).

Canadian carrier (as defined in the *Telecommunications Act*): A person who owns or operates a transmission facility used by that person or another person to provide telecommunications services to the public for compensation.

Customer: A person who subscribes to the carrier's services that are subject to the blocking.

Cyber security: A body of technologies, processes, practices, and response and mitigation measures designed to protect against cyber attacks in order to ensure confidentiality, integrity, and availability of electronic information.

Cyber attack: Malicious use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.

False positive: Occurs when non-malicious content is incorrectly blocked.

Indicator of compromise: An identifier used by carriers to block network traffic for cyber security purposes that indicates, with a high degree of confidence, intrusion on a system and that malicious activity is occurring. In other words, an IOC is a technical characteristic of a particular cyber attack. In the context of a blocklist, an IOC may consist of, for example (i) a domain name or (ii) an IP address and port number.

Over-blocking: Blocking applied to malicious traffic in an overly broad manner or to benign content.

Reporting period: The calendar year from 1 January to 31 December (12 months), with the first reporting period beginning on the day that section 7.0 of the framework comes into effect and ending on 31 December of that year.

****

Pursuant to section 36 of the *Telecommunications Act*, the Commission authorizes Canadian carriers to take cyber security measures to block Internet traffic crossing their networks, solely for the purpose of protecting against cyber attacks, subject to

compliance with the terms and conditions set out below. The terms and conditions, except the requirements in section 7.0, will come into effect on **12 August 2025**. Section 7.0 will be effective upon approval of the final blocking framework.

This authorization does not apply to the blocking of traffic for any other purpose, including blocking otherwise illegal activity, or blocking for commercial, competitive, or political purposes.

1.0. Blocking by default

1.1. Blocking must operate at the network level by default: a customer cannot opt in or opt out.

1.2. The carrier must not, however, implement any measure that may prevent customers from employing legitimate services that may circumvent the blocking, such as virtual private network services or alternative Domain Name System resolvers.

2.0. What is authorized to be blocked and how

2.1. The carrier may only block malicious Internet traffic based on indicators of compromise (IOCs) that are listed on an Authorized Blocklist, as identified in section 2.2.

2.2. Subject to a carrier's compliance with the requirements set out in this section and sections 3.0 and 4.0, the Authorized Blocklists that the carrier is permitted to use are the following:

(a) a third-party blocklist that may be made available to a carrier through any automated method or platform of their choice; and

(b) a carrier's in-house, proprietary blocklist.

2.3. The carrier may use one or more Authorized Blocklist(s), in whole or in part, to the best extent of its technical capacity.[1]

2.4. The carrier must use an Authorized Blocklist in the manner specified by its provider (e.g., the provider may specify a particular update frequency to ensure proper expiry of IOCs). However, in the event of conflict, the terms and conditions imposed herein by the Commission prevail over any conflicting requirements of a blocklist provider.

---

[1] This technical capacity may be limited, for example, in terms of the volume of IOCs to be blocked (limits in computing resources) or in terms of the nature of IOCs and the layer of the Open Systems Interconnection (OSI) model at which blocking is performed. As a result, any Authorized Blocklist may be reduced or customized by the carrier.

3.0. Third-party blocklist

3.1. A carrier may only use a third-party blocklist if it is satisfied that the blocklist and its provider meet, at a minimum, the following criteria:

(a) The blocklist provider has the necessary technical expertise, as demonstrated, for example, by years of activity in researching new and changing cyber threats, by market acceptance and certified endorsement of industry professionals, or by certifications to well-known International Organization for Standardization (ISO) or other standards.

(b) The blocklist provider has no potential conflict of interests (e.g., ownership and geopolitical context) that may compromise the operation of its blocklist in an unbiased manner and in the best interest of Canadians.

(c) The common requirements set out in section 4.0 are met.

4.0. Requirements applicable to all Authorized Blocklists

4.1. A carrier may only use an Authorized Blocklist that complies with the following minimum criteria:

(a) The blocklist only identifies IOCs that are related to cyber attacks.

(b) The blocklist provider has the capacity to receive IOCs from third parties.

(c) The blocklist provider has a mechanism in place to be able to verify whether each IOC on the list is malicious and to assess it for collateral damage. The blocklist provider has a mechanism in place to ensure that any impact the blocking may have on legitimate services is as low as possible, strictly limited to that which is necessary to achieve the objective of blocking the malicious traffic.

(d) The blocklist is continually updated using, for example, a mix of manual review, automated IOC delisting, or expiry dates.

(e) The blocklist provider has a process in place, with service standards, for responding to false-positive or over-blocking complaints. At a minimum, the complaints process must involve

(i) a review of the IOC at issue;

(ii) updates to the blocklist where required to remove the IOC from the blocklist (in the case of a false positive) or to substitute a more specific IOC (in the case of over-blocking); and

(iii) reporting back to the originating carrier, in a timely manner, the action taken, in compliance with the requirements set out in section 5.2.

5.0. Accuracy (false positives and over-blocking)

5.1. Upon receipt of a customer complaint regarding a potential false positive or over-blocking, the carrier must determine whether the root cause is due to a blocklist subject to this framework and, if so, send the complaint to the blocklist provider.

5.2. The carrier must resolve a complaint within two business days of its receipt in one of the following two ways:

(a) if a false positive or over-blocking is confirmed, the carrier must update the blocklist, as set out in section 4.1(e)(ii) above (i.e., unblocking); or

(b) if the IOC is confirmed as malicious and the blocking is maintained, the carrier must notify the customer.

6.0. Transparency (disclosure requirements)

6.1. The carrier must disclose, clearly and prominently on its website, information about the cyber security blocking occurring under this framework. This information must be identified with a distinct "cyber security blocking" heading.[2] The carrier must also reference its online disclosures in relevant marketing materials, customer contracts, and terms of service.

6.2. The online disclosure must provide sufficient, plain-language information for Canadians to understand the type and scope of blocking that is in place; when and how it will be applied; the process for filing and investigating complaints related to potential false positives and over-blocking; and any relevant privacy-related information and necessary statements. At a minimum, the following information must be included to meet that requirement:

(a) That the blocking follows the terms and conditions set out in *Development of a framework to limit botnet traffic*, Compliance and Enforcement and Telecom Decision CRTC 2025-142, 13 June 2025. Therefore, the blocking is done exclusively for the purpose of protecting against cyber attacks and not for any other purpose, such as blocking other illegal activities or blocking for commercial, competitive, or political purposes. The purpose is to protect customers' computers from malicious botnets (i.e., from joining a network of malware-infected devices controlled by a threat actor without the customers' knowledge and consent) and from other cyber threats including malware and phishing. The blocking does not involve any appreciation of the content of visited websites. For example, this blocking does not contemplate websites

[2] This information may be published on the same webpage as the information disclosed pursuant to the Commission's existing requirements related to Internet traffic management practices or at any other relevant location.

offering illicit goods or services, or websites publishing false or misleading news, abusive comments, or obscene material.

(b) That the blocking is applied at the network level by default, which means that customers may not request to opt in or opt out.

(c) The type of blocking that is being used (i.e., a blocking based on a blocklist of indicators which have been vetted as being malicious) and the type of indicator being used for this purpose (e.g., IP address, IP address and port number, or domain name).

(d) The carrier's contact information for filing complaints and the process that will be followed.

(e) That the blocking aims to provide a safer Internet service, but it is not a replacement for user-level protections: service providers provide cyber security protections for their networks and consumers provide cyber security protections for their own devices. Therefore, it is important that customers continue to secure their devices and their Internet connection against cyber threats (e.g., by installing and updating antivirus software, performing regular software updates, managing a firewall, using strong passwords, enabling two-factor authentication, and securing their wireless connection).

6.3 If a carrier implements a new blocking mechanism or modifies an existing one, it must comply with the disclosure requirements of this section at least 30 days before the change.

6.4. Online disclosure is to be made accessible for persons with disabilities in a manner consistent with the accessibility determinations outlined in *Accessibility of telecommunications and broadcasting services*, Broadcasting and Telecom Regulatory Policy CRTC 2009-430, 21 July 2009, as amended by Broadcasting and Telecom Regulatory Policy CRTC 2009-430-1, 17 December 2009.

7.0. Transparency (performance metrics)

(Section 7.0 will be effective upon approval of the final blocking framework)

7.1. The carrier must file the following information with the Commission,[3] regarding the blocklist(s) it used over the reporting period, within 30 calendar days of the end of each reporting period:

(a) Identification of all the blocklists used by the carrier (whether from a third party or in-house), including the name of the provider and the name of the blocklist.

(b) If a blocklist is not used through the entire reporting period, the implementation starting date and ending date. If a third-party blocklist is not used in its entirety but only in part, details regarding how customization is applied.

(c) The total number of unique IOCs effectively blocked by the carrier, including a breakdown by number of unique (i) IPs, (ii) domains, and (iii) other types of IOCs.

(d) The total number of blocking events, including a breakdown by type of cyber threat: (i) botnet, (ii) malware, (iii) phishing, and (iv) other cyber threats.

(e) Regarding the IOCs detected and blocked using an in-house blocklist, the total number of unique IOCs that are not within the carrier's network, and the total number that have been shared with other carriers to mitigate the corresponding threat on other networks, as well as the method used for sharing (i.e., automated or manual).[4]

(f) The total number of notifications sent to customers to warn them that their computer has been infected.[5]

(g) The number of blocking events per subscriber per month (i.e., the total number of blocking events [from section 7.1.d] divided by the total number of Internet subscribers divided by the number of months in the reporting period). Include all figures used to derive the per-subscriber number.

(h) The total number of false-positive or over-blocking complaints received from customers for each blocklist in use and the total number of false-positive and over-blocking events that were confirmed.

---

[3] Regarding the submission method, refer to the webpage Submitting applications and other documents to the CRTC using My CRTC Account.

[4] In accordance with sections 3.1.4 (#11) and 6.1 of *Security Best Practices for Canadian Telecommunications Service Providers (TSPs)*, Canadian Security Telecommunications Advisory Committee (CSTAC), 31 October 2013 (CSTAC Security Best Practices).

[5] In accordance with sections 5 and 6 of *Recommendations for the Remediation of Bots in ISP Networks*, Request for comments (RFC) 6561, the Internet Society (Internet Engineering Task Force), March 2012, and section 5.2.1 of CSTAC Security Best Practices.

(i) A hyperlink to the webpage used to meet the disclosure requirements set out in section 6.0.

(j) If a carrier uses an in-house blocklist, a detailed description of how each in-house blocklist operates including, for example, reference to the requirements set out in section 4.1.

8.0. Accountability and privacy

8.1. The carrier must periodically review all its blocking systems subject to this framework to verify that they work as intended.

8.2. If the carrier collects, uses, or intends to disclose personal information for the purpose of the activities performed under this framework, the carrier must fully comply with all applicable laws and regulations pertaining to the protection of personal information. This framework does not permit any additional collection, use, or disclosure of personal information.

9.0. Other conditions

9.1. The carrier must comply with any other conditions that the Commission may establish from time to time following a public process.