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

Telecom Regulatory Policy CRTC 2017-91

PDF version

Reference: Telecom Notice of Consultation 2016-115

Ottawa, 6 April 2017

File number: 1011-NOC2016-0115

Implementation of the National Public Alerting System by wireless service providers to protect Canadians

*The Commission **directs** wireless service providers to implement wireless public alerting capability on their long-term evolution networks by 6 April 2018. Concurrent with this implementation, the Commission **directs** the CRTC Interconnection Steering Committee (CISC) to resolve a number of outstanding issues before the mandatory distribution of emergency alert messages begins. Among these issues is the creation of a public awareness campaign to ensure that Canadians are fully informed about this new initiative.*

Alerts on mobile devices will warn Canadians about dangers to life and property in a timely manner so that they can take appropriate action. The Commission expects that this new capability will be available in approximately 12 months.

Introduction

1. Emergency alert messages are issued by public officials designated as emergency management officials (EMOs) for immediate distribution to the public to warn of dangers to life and property. These messages contain information relating to the nature of the threat, the area affected, and actions the public should take.

2. In 2009, the Commission mandated Pelmorex Communications Inc. (Pelmorex) to create an emergency alerting system (the National Alert Aggregation & Dissemination [NAAD] System) by mid-2010.[1] The NAAD System is at the core of Canada's National Public Alerting System (NPAS). Participation by broadcasters at that time was strictly on a voluntary basis.

3. Due to a lack of voluntary participation by broadcasters, in 2014 the Commission required all broadcasters and broadcasting distribution undertakings (BDUs), with very limited exceptions, to participate in the NPAS.[2]

[1] See Broadcasting Order 2009-340.

[2] See Broadcasting Regulatory Policy 2014-444.

4. Recognizing the growing importance of wireless services in Canadians' everyday lives and the potential to notify a greater number of Canadians of imminent or unfolding dangers, in Telecom Notice of Consultation 2016-115 (the Notice), the Commission issued a call for comments regarding participation by wireless service providers (WSPs) in the NPAS.

5. The Commission asked for comments on, among other things, whether all Canadian WSPs (including primary brands, extensions brands, and resellers) should be required to participate in wireless public alerting (WPA) and, if so, the costs and timelines associated with the cost of implementing WPA, whether alerts should be based on existing standards, and whether monitoring and compliance measures should be put in place.

6. The Commission received interventions from a wide range of parties, including individuals; EMOs; municipal, regional, and provincial governments; industry groups; non-profit organizations; technology solution providers; WSPs; the Canadian Wireless Telecommunications Association (CWTA); the Office of the Privacy Commissioner of Canada (OPC); and the Senior Officials Responsible for Emergency Management Federal/Provincial/Territorial Public Alerting Working Group (SOREM).[3] The public record of this proceeding, which closed on 25 July 2016, is available on the Commission's website at www.crtc.gc.ca or by using the file number provided above.

Issues

7. The Commission has identified the following issues to be addressed in this decision:

- Mandatory participation and exemptions
- Costs
- Liability
- Mandatory receipt of emergency alert messages
- Standards, technology, and related issues
- Test message schedule and parameters
- Awareness campaign
- Governance

[3] SOREM is a federal/provincial/territorial body that works to harmonize and improve emergency practices across the country. It includes representatives from provincial and territorial emergency management organizations as well as Public Safety Canada.

- Implementation timeline and monitoring

Mandatory participation and exemptions

Mandatory participation

8. The Commission sought comments on whether participation in WPA should be mandatory for all Canadian WSPs and imposed as a condition of service under sections 24 and 24.1 of the *Telecommunications Act* (the Act).[4]

9. The majority of interveners, including several EMOs, WSPs, technology solution providers, individuals, and the CWTA, submitted that WSPs should be required to participate in WPA.

Commission's analysis and determinations

10. One of the Canadian telecommunications policy objectives set out in section 7 of the Act is to facilitate the orderly development throughout Canada of a telecommunications system that serves to safeguard, enrich, and strengthen the social and economic fabric of Canada and its regions.[5]

11. According to the 2016 CRTC *Communications Monitoring Report*, Canadians are increasingly shifting toward mobile devices for their communications needs. More Canadian households reported subscribing to mobile telephone services (85.6%) than to landline telephone services (75.5%). In addition, the number of wireless service subscribers increased to nearly 30 million in 2015.

12. In light of the above, and consistent with the Commission's earlier determination to require broadcasters and BDUs to participate in the NPAS, requiring WSPs to distribute emergency alert messages on mobile devices would be in the public interest and would help protect Canadians from imminent threats to life and property. This approach is consistent with a number of countries that have implemented public alerting on mobile devices.

---

[4] Section 24 of the Act states that the offering and provision of any telecommunications service by a Canadian carrier are subject to any conditions imposed by the Commission or included in a tariff approved by the Commission. Section 24.1 of the Act states that the offering and provision of any telecommunications service by any person other than a Canadian carrier are subject to any conditions imposed by the Commission, including those relating to (a) service terms and conditions in contracts with users of telecommunications services; (b) protection of the privacy of those users; (c) access to emergency services; and (d) access to telecommunications services by persons with disabilities.

[5] See paragraph 7(a) of the Act.

13. Accordingly, the Commission determines that, as a condition of service under sections 24 and 24.1 of the Act, all Canadian WSPs (i.e. both carriers and non-carriers)[6] are required to participate in the NPAS.

Exemptions

14. Many EMOs requested that WPA be deployed on all cellular networks, and that a technology be chosen that supports all mobile devices in use today.

15. All WSPs that submitted interventions in the proceeding stated that implementing WPA on their pre-long-term-evolution (LTE) networks would add considerable time and cost. WIND Mobile Corp., now known as Freedom Mobile Inc. (Freedom Mobile), referred to its third-generation (3G) / evolved high-speed packet access (HSPA+) network as "legacy," while Rogers Communications Canada Inc. (RCCI) indicated that its second-generation (2G) and 3G networks are nearing the end of their operational lives.

16. Two mobile satellite service providers, TerreStar Solutions Inc. and Ligado Networks, submitted that issuing alerts over satellite networks is technically infeasible, since satellite beams serve large areas, making precise geo-targeting impossible. The two companies indicated that exempting mobile satellite service providers from a WPA mandate would be similar to their exemption from Enhanced 9-1-1 (E9-1-1) and emergency alerting in the United States.

Commission's analysis and determinations

17. The 2016 CRTC *Communications Monitoring Report* indicates that approximately 97.4% of the Canadian population has access to an LTE network. Further, WSPs continue to deploy and expand their LTE networks.

18. The Commission stated in Telecom Regulatory Policy 2016-496 that "the latest generally deployed mobile wireless technology [LTE technology] should be available in Canada not only in premises, but on as many major transportation roads as possible" and announced a fund to help support the continued rollout of these technologies in underserved areas. The Commission is of the view that exempting pre-LTE networks from WPA requirements will have minimal impact on the coverage of emergency alerting. Conversely, requiring WPA on pre-LTE networks would increase deployment costs and delay the deployment of emergency alerts over wireless networks.

19. The term "wireless service provider," as used by the Commission, does not encompass mobile satellite services, and thus the obligation regarding WPA would not apply to these services. The Commission recognizes that many communities in

---

[6] A carrier is a person who provides telecommunications services to the public over facilities that it owns or operates, and whose services are subject to conditions pursuant to section 24 of the Act. A non-carrier is a person who provides telecommunications services to the public but who is not a carrier, and whose services are subject to conditions pursuant to section 24.1 of the Act.

the North depend on mobile satellite service where no terrestrial networks exist. However, the inability to undertake precise geo-targeting due to the nature of satellite beams would make the rollout of WPA on mobile satellite service technologies impractical. Further, there is widespread AM and FM radio coverage in the North, and residents will continue to receive emergency alert messages over these stations.

20. In light of the above, the Commission will not require the implementation of WPA on pre-LTE networks or mobile satellite services.

Costs

21. Interveners had a variety of opinions regarding how to cover costs for WPA, including an annual fee charged to wireless service customers and federal funding. Overall, WSPs indicated that the implementation and maintenance of WPA would create new capital and operating costs, and that all costs must ultimately be recovered through the provision of services. They submitted that WPA would be offered to the Canadian population and that, therefore, the costs should be borne by all users. RCCI indicated that it would not add additional charges to its subscribers' invoices to cover, in whole or in part, the costs of implementing and maintaining WPA.

Commission's analysis and determinations

22. The Commission does not regulate wireless rates. The information that WSPs submitted indicates that WPA implementation costs, as well as operational and maintenance costs, would result in nominal costs on a per-customer basis.

23. Nevertheless, it would not be appropriate for WSPs to identify a separate fee for WPA service on subscribers' bills.

24. In light of the above, the Commission determines, as a condition of service under sections 24 and 24.1 of the Act, that WSPs may not identify a separate fee for WPA on subscribers' bills.

Liability

25. Bell Canada, the CWTA, and RCCI submitted that WSPs should receive liability indemnification during the course of providing all emergency services, including any liability arising from the delivery of emergency alert messages as part of WPA.

26. They submitted that in past decisions, the Commission has recognized the principle that WSPs should be provided liability indemnification when providing mandated emergency services. They submitted that the regulatory framework for WPA should contain a similar provision to the one set out in Telecom Decision 2003-53, in which the Commission established the conditions for WSPs' E9-1-1 services and set out limitation of liability provisions to apply to wireless carriers in respect of emergency services provided to end-users on a mandatory basis.

Commission's analysis and determinations

27. With respect to wireless services, the Commission has forborne from exercising its powers under section 31 of the Act,[7] which pertains to limitations of liability and which reads as follows: "No limitation of a Canadian carrier's liability in respect of telecommunications service is effective unless it has been authorized or prescribed by the Commission." As such, carriers are free to set limitations of liability without Commission approval, subject to laws of general application (e.g. contract or torts laws).[8]

28. In the case of E9-1-1, in Telecom Decision 2003-53, the Commission determined that because it was mandating the provision of E9-1-1 services, and because wireless carriers could be subject to claims in regard to their provision of those services, it would reinstate its powers pursuant to section 31 of the Act to the limited extent necessary to provide liability protection with respect to the provision of the mandated services. Wireless carriers were directed to include a specified provision in their end-user service contracts.

29. In the broadcasting context regarding the dissemination of emergency alert messages, the Commission indicated that liability for the content of emergency alert messages lies with the originator of the message and that issues pertaining to liability should not prevent the participation of last-mile distributors (e.g. BDUs and broadcasters) in the NPAS.

30. By reapplying section 31 of the Act in respect of the participation of WSPs in WPA, the Commission could ensure comparable limitation of liability across all wireless carriers. However, providing indemnification of liability to WSPs would be inconsistent with the Commission's approach in the broadcasting context, where it required participation in emergency alerting despite parties' concerns about liability. It expected parties to work together to resolve outstanding issues relating to liability. BDUs have been participating in emergency alerting for years (e.g. in Alberta), and participating in Commission-mandated emergency alerting for almost two years, without indemnification of liability.

31. Without any Commission action, WSPs would still be able to include their own legitimate limitation of liability clauses in end-user contracts, to the extent permitted by laws of general application.

32. In light of the above, the Commission determines that it is not appropriate to reapply section 31 of the Act in these circumstances as WSPs can limit their liability to the extent permitted under laws of general application. Moreover, the Commission

---

[7] In Telecom Decision 96-14, the Commission forbore from exercising its powers under various sections of the Act with regards to mobile wireless telecommunications service.

[8] Section 31 of the Act does not apply to resellers; like forborne carriers, resellers are permitted to set limitations of liability, without needing Commission authorization.

reiterates that liability for the content of emergency alert messages lies first and foremost with the originator of the message.

Mandatory receipt of emergency alert messages

33. The Commission sought comments on whether the receipt of emergency alert messages should be mandatory, or whether individual users should have the choice to opt out of receiving such alerts or silence them on their mobile devices.

34. SOREM has established a definitive list of emergency alert message types for immediate broadcast by alert distributors. These messages are defined as “Broadcast Immediately” (BI).

35. Individual interveners’ views were divided among mandatory receipt, an opt-in mechanism, and the choice to opt out. Technology solutions providers indicated mixed support between mandatory reception and the choice to opt out. EMOs strongly supported mandatory receipt.

36. The OPC submitted that many people consider their mobile devices to be private and personal, and that some individuals could consider emergency alerts to be intrusive. It recommended that the Commission review how opt-out mechanisms have been implemented in the United States and other jurisdictions, and whether the ability to opt out has had a significant negative effect on alerting individuals in an emergency situation. It submitted that individuals should be allowed to opt out if the effect is found to be minimal.

37. Most WSPs submitted that users should have the ability to opt out or disable the ring tone and vibration for certain types of alerts. Although RCCI supported the capability for subscribers to opt out of receiving emergency alert messages, it suggested that a list of alerts for WPA should be addressed and maintained by an expanded NAAD System Governance Council (the Governance Council), which would follow the CRTC Interconnection Steering Committee (CISC) Administrative Guidelines for all stakeholders to arrive at a consensus.

38. Bragg Communications Incorporated, operating as Eastlink (Eastlink), submitted that the receipt of emergency alert messages should be mandatory and that customers should not be permitted to opt out.

39. Some WSPs provided insight on past experiences regarding the distribution of AMBER Alerts over their parent BDUs. For example, in March 2016, the Ontario Provincial Police issued an AMBER Alert, which was distributed by BDUs. Many television viewers were upset by the interruption of their television viewing and contacted their BDU customer service centres and, in some cases, 9-1-1 to complain.

40. In response to a Commission request for information regarding whether all current BI alerts should be sent to mobile devices (i.e. that they should use the same BI list), or whether a new subcategory for WPA should be defined, there was support for

both options. Some interveners also suggested modifying the BI list to adapt it for WPA.

Commission's analysis and determinations

41. Although some interveners suggested modifying the BI list, there was no consensus on which specific categories should be added or removed.

42. However, the question in this proceeding is not whether the BI list used in the broadcasting context should be changed, but whether the same or a different approach should be taken with respect to emergency alert messages sent to mobile devices compared to those sent via broadcasting emergency alerting. The current BI list is designed to protect against threats to life and property. It is therefore important to promote consistency between broadcasting and wireless emergency alerts so that Canadians can receive the same alerts regardless of transmission medium.

43. In light of the above, the Commission mandates the reception of emergency alert messages on mobile devices, based on the BI list developed by SOREM, as amended from time to time.

Standards, technology, and related issues

Standards and technology

44. There are two complementary standards that define a set of functional and technical requirements for WPA in Canada:

    - The NPAS Common Look and Feel (CLF) Guidance was developed by SOREM for emergency alert messages. The CLF Guidance sets out the current collection of specifications, policy decisions, and recommended practices associated with the NPAS. It was developed to ensure uniformity and consistency throughout all alerting media.
    - ATIS[9] 0700021[10] (the ATIS standard) is a standard developed for Canada that defines a set of requirements for the behaviour of WPA-capable mobile devices whenever a wireless emergency alert message transmitted over an LTE network is received. This standard complies with the CLF Guidance.

45. Two types of technology have been tested in Canada as possible solutions for the provision of WPA: Cell Broadcast (CB)[11] technology and location-based Short

---

[9] ATIS (the Alliance for Telecommunications Industry Solutions) is a standards-setting body based in the United States. Telecommunications equipment manufacturers use its standards to ensure common functionality and interoperability.

[10] *Canadian Wireless Public Alerting Service (WPAS) LTE Mobile Device Behavior Specification*

[11] With this technology, emergency alert messages are automatically broadcast to and received by all cell phones simultaneously in the vicinity of cell towers in an area subject to an alert.

Message Service (LB-SMS)[12] technology. The ATIS standard specifies the use of CB technology.

46. In the Notice, the Commission sought comments on whether emergency alert messages should be based on the CLF Guidance, the ATIS standard, or another standard or combination of standards.

Positions of parties

47. Many EMOs provided general comments, stating that WPA could follow functional or technical requirements.

48. The Calgary Emergency Management Agency, Comtech TCS (Comtech), and South Central Emergency Management supported the use of the CLF Guidance for WPA.

49. TELUS Communications Company (TCC) did not specify which technology it preferred, but stated its support for the implementation of a single WPA system in Canada. It also recommended that the Commission's final decision include any recommendations already made by CISC in the development of WPA requirements. The Commission should also take into account the outcome of a public WPA trial based on CB technology that was carried out by the Defence Research and Development Canada Centre for Security Science in Durham Region.

50. Bell Canada submitted that adhering to the ATIS standard would reduce handset development time and overall implementation costs.

51. Pelmorex submitted that the NAAD System could support WPA on a national scale if WPA using CB technology were implemented.

52. EMOs in general, technology solutions provider Mobilaris AB (Mobilaris), Bruce Power, and one individual expressed a preference for LB-SMS. Bruce Power indicated that this technology could reach all Canadian mobile devices today by using text messaging, whereas CB would require a compatible handset. While these parties expressed preference for LB-SMS, they did not indicate an equivalent to the ATIS standard that uses LB-SMS technology and meets the CLF Guidance.

Commission's analysis and determinations

53. It is important to take into account the user experience when developing an emergency alerting system, as well as to strive towards uniformity and consistency throughout all alerting media (broadcasting and mobile wireless).

54. SOREM has defined 36 requirements for WPA with the goal of maintaining uniformity and consistency throughout all alerting media (broadcasting and mobile

---

[12] With this technology, emergency alert messages are sent to each cell phone individually via standard text messaging in an area subject to an alert.

wireless). The ATIS standard meets all elements of the CLF Guidance for broadcasting emergency alerts.

55. In light of the support for the ATIS standard, the lack of an LB-SMS standard, and the importance of ensuring uniformity and consistency throughout all alerting media, it would be appropriate for the ATIS standard and the CLF Guidance to be adopted. Accordingly, the Commission mandates the reception of emergency alert messages on mobile devices that respect the ATIS standard and the CLF Guidance, as amended from time to time.

56. While the Commission asked in the Notice whether it should mandate the use of a specific technology, the ATIS standard is written specifically for CB technology over LTE networks. Therefore, there is no further need to address a specific technology.

Authenticity of emergency alert messages

57. The Commission requested comments on how Canadians could be assured of the authenticity of emergency alert messages received on their mobile devices.

58. Technology solution providers one2many and Unified Messaging Systems ASA indicated that authenticity is an inherent characteristic of CB technology, since CB messages can only be sent by WSPs. Individuals cannot use CB to send messages, unlike SMS messages which can be sent between individuals. Furthermore, SMS messages are not exclusively emergency alert messages and will be mixed with other SMS messages. However, Mobilaris submitted that WSPs have anti-spoof technology for SMS messages.

59. The Province of British Columbia and Halton Region indicated that the use of guidelines such as the CLF Guidance can ensure the authenticity of emergency alert messages.

60. The CWTA and WSPs indicated that using the ATIS standard would provide assurance regarding the authenticity of emergency alert messages. RCCI submitted that the standard sets specifications for the alert tone, vibration, and banner, which are unique to Canadian WPA, thus ensuring authenticity.

61. Freedom Mobile submitted that the CLF Guidance was not sufficient to ensure the authenticity, but could be used in conjunction with the ATIS standard to distinguish legitimate emergency alert messages. Freedom Mobile and TCC also submitted that authenticity could be enhanced through an education campaign to help Canadians easily recognize a WPA message.

62. Mobility & Wireless Solutions Inc. (MWSI), the contractor for the Durham Region CB pilot project, submitted that with LB-SMS, the public cannot be certain that an emergency alert message was sent by an authorized alerting authority. WSPs argued that there is no way to guarantee the authenticity of an SMS message, and that SMS technology remains vulnerable to spoofing, despite Mobilaris’s claim.

Commission's analysis and determinations

63. Since WPA messages have the potential to reach a higher number of Canadians than broadcasting emergency alert messages, it is important that Canadians be assured of the authenticity of such messages. Regardless of the technology, the public can verify the validity of a WPA message through an official website (e.g. Pelmorex or a provincial government website), a broadcasting emergency alert message, or another person with a mobile device in their vicinity. Nonetheless, confirming the authenticity of a WPA message should not be the responsibility of the recipient. Canadians should have a WPA system that is trustworthy and that assures them of the authenticity of emergency alert messages received on their mobile devices.

64. LB-SMS messages are vulnerable to spoofing and, as WSPs submitted, there is no known reliable manner to mitigate this, regardless of the views of Mobilaris.

65. Directing the industry to adopt standards such as the ATIS standard will ensure that Canadians can be assured of the authenticity of WPA messages. A specific banner and the Canadian Alerting Attention Signal and vibration cadence will validate the authenticity of the message. Accordingly, there is no need to set additional provisions related to message authentication.

66. In light of the above, the Commission is of the view that the adoption of the ATIS standard will assure Canadians of the authenticity of emergency alert messages received on their mobile devices. Accordingly, the Commission mandates the reception of emergency alert messages on mobile devices that respects the ATIS standard, as amended from time to time.

Privacy

67. Several interveners raised the issue of privacy in relation to the technology used for WPA.

68. The OPC submitted that unlike LB-SMS, CB technology does not require determining which mobile telephone numbers are present in a given area, and therefore does not require the collection of any additional personal information such as location. However, the OPC cautioned that regardless of which technology is chosen, safeguards are required to ensure that no information about which devices have been sent an emergency alert message or the location of those devices should be retained. As well, it submitted that reports of the number of messages sent should not include information on which users (i.e. mobile telephone numbers) received the messages.

69. Technology solution provider one2many submitted that privacy is basically a non-issue when using CB, since the distribution of emergency alert messages to mobile devices is done with one-way communication.

70. Two individual interveners submitted that individual privacy and rights cannot take precedence over the safety and security of the majority.

Commission's analysis and determinations

71. While LB-SMS, as opposed to CB, requires the collection of mobile telephone numbers, the root of the privacy concern is having a list of these numbers tied to individuals to a particular geographic location at a specific time. Most Canadians would not likely have an issue with their mobile telephone number being tied to their billing address, since their WSP already has this information. However, Canadians might be more likely to perceive being tracked if their physical location was known as a derivative of WPA.

72. The courts have confirmed that Canadians have a reasonable expectation of privacy in the records of their mobile device activities, and the location of a person at a particular time raises privacy concerns.[13]

73. Although Phase II E9-1-1 service uses device location, there are different privacy implications between WPA and E9-1-1. In the situation of a 9-1-1 emergency call on a mobile device, the individual requesting assistance initiates this communication; therefore, it is reasonable to assume that they would want their location known in order to be found by first responders. There is also the possibility that the caller does not know their exact location, and automatically enabling the Global Positioning System (GPS) on the device and transferring their location to the appropriate resource will decrease response time. In contrast, a user who receives an emergency alert on a mobile device does not initiate this communication and might not want the GPS location of their mobile device to be known.

74. In the Commission's view, adoption of the ATIS standard will lead to the deployment of a more privacy-sensitive WPA technology that does not require the geolocation of Canadians' mobile devices. Accordingly, to address privacy concerns, the Commission mandates the reception of emergency alert messages on mobile devices that respects the ATIS standard, as amended from time to time.

Test message schedule and parameters

75. SOREM currently recommends five tests per year for broadcasting emergency alerts: four quarterly tests, and one test during Emergency Preparedness Week. In the Notice, the Commission sought comments on whether there should be a testing schedule for WPA, and if it should coincide with the broadcasting test schedule.

76. EMOs, technology solution providers, and WSPs generally agreed that testing is important, and that it should coincide with the broadcasting test schedule.

77. Bell Canada and RCCI submitted that test messages could be sent on a separate CB channel, where users would have the choice to opt in to receive test messages.

---

[13] See, for instance, *R. v Rogers Communications*, 2016 ONSC 70. This case involved Production Orders that the Peel Regional Police served on RCCI and TCC, requesting the names and addresses of all users whose mobile devices connected to certain cell towers.

Initially, test messages could be sent over the mandatory reception channel (currently used for all BI alerts) for public awareness, then sent through the test channel only, so the messages would be invisible to users who have not opted in.

78. Bell Canada and TCC submitted that if too many test messages are sent, it could potentially lead mobile device users to mistake real alerts for tests, which would greatly reduce the overall effectiveness of WPA.

79. MWSI submitted that five test alerts per year over the public channel would result in alert fatigue, and recommended that the Commission consider working with SOREM to conduct testing over a test channel.

80. An individual intervener in Durham Region, who did not participate in the CB trial but had a Wireless Emergency Alert-enabled[14] mobile device, submitted that he had been receiving alerts on his mobile telephone but had no way to stop them or turn them off or down. He indicated that this was unacceptable.

Commission's analysis and determinations

81. As written, the ATIS standard does not include a mechanism for users to opt out of the five tests per year that SOREM recommends. This means that individuals would receive BI alerts on their mobile devices a minimum of five times per year in the absence of any real emergencies. In contrast, the Federal Communications Commission in the United States requires participating carriers to conduct periodic tests, but alerts that are sent as part of the testing process are delivered on a separate opt-in channel. If users do not choose to receive test alerts, the testing process is invisible to them.

82. The Commission is of the view that only one test alert per year should be sent over the mandatory reception channel during Emergency Preparedness Week, and that all other test alerts should be sent over the test channel. However, given that the creation of a test message schedule and frequency of test message distribution will require collaboration between WSPs and EMOs, and potentially will require amendments to the ATIS standard, the Commission considers CISC to be the appropriate forum to obtain consensus and accomplish the necessary work. In particular, CISC's Network Working Group is familiar with WPA, having worked on the WPA system technical specifications, and having carried out the prerequisite work for creation of the ATIS standard. Further, CISC membership is open, so EMOs could work alongside WSPs toward a consensus.

83. In light of the above, the Commission requests that CISC report back to the Commission, with a progress report by **5 July 2017**, and a final report by **3 October 2017** on the following:

---

[14] Wireless Emergency Alerts – formerly known as the Commercial Mobile Alert System (CMAS) – is the United States' WPA system; it is based on CB technology.

- a public awareness test schedule, which includes only one visible alert per year during Emergency Preparedness Week;
- a frequency and schedule for test alerts that are invisible to end-users; and
- amendments to the ATIS standard as required.

84. The Commission encourages EMOs and SOREM to participate in the CISC process.

Awareness campaign

85. In Broadcasting Decision 2011-438, Pelmorex was directed to develop and fund a public awareness and education campaign to prepare Canadians for the introduction of the NPAS (the Alert Ready campaign). The expansion of the NPAS to include WSPs will be a major evolution in how the public receives emergency alert messages.

86. In the Notice, the Commission sought comments on whether an awareness campaign is necessary to educate the Canadian public about WPA, and who should be responsible for such a campaign.

Positions of parties

87. All parties agreed that there should be an awareness campaign for WPA to ensure that Canadians understand the new alerting process and what to do when an emergency alert message is received. A number of them submitted that a significant awareness campaign will be required, and that a failure to have one would reduce the effectiveness of WPA. Several interveners suggested that a WPA awareness campaign should be similar to, if not an extension of, the Alert Ready campaign.

88. Some interveners suggested that a WPA awareness and education campaign be developed under the responsibility of the federal, provincial, and territorial governments, since those governments are responsible for sending emergency alert messages.

89. MWSI indicated that it had received comments from the Federal Emergency Management Agency (FEMA) and American WSPs. The feedback from these two sets of United States stakeholders highlighted that the lack of a public awareness campaign in the United States resulted in a number of unhappy customers and some embarrassment for FEMA.

Commission's analysis and determinations

90. A WPA awareness and education campaign should be a coordinated effort between SOREM, federal, provincial, and territorial EMOs, WSPs, the NAAD System administrator, and the Commission. However, the Commission did not receive fulsome responses regarding certain elements of an awareness campaign, such as the content of the campaign, the timeline, delivery mechanisms, and funding. Considerable coordination among all stakeholders will be required and, therefore, the

Commission is of the view that CISC would be the most appropriate forum to address this issue.

91. Accordingly, the Commission requests that CISC report back to the Commission, with a progress report by **5 July 2017**, and a final report by **3 October 2017**, with recommendations on a WPA awareness and education campaign. The reports should include the following information:

    - who should be responsible for the campaign;
    - what material the campaign should include;
    - how the campaign should be funded;
    - how the campaign should be delivered; and
    - when the campaign should start.

92. The Commission encourages EMOs and SOREM to participate in the CISC process.

93. Given that the obligation to distribute alerts only applies to LTE networks, the Commission **directs** WSPs, as part of the campaign, to notify their subscribers with non-LTE-compatible handsets that they will be unable to receive emergency alert messages on their mobile devices.

Governance

94. The Governance Council oversees the operation of the NAAD System, and includes representation from EMOs, SOREM, Pelmorex, broadcasters, and BDUs. As part of this proceeding, a number of parties commented on the need to develop an overall governance structure or forum for both types of emergency alerting.

95. SOREM signalled its intent to explore governance mechanisms in consultation with public alerting stakeholders, such that WSPs could be included in a future multi-stakeholder governance model.

96. A number of interveners commented on the shortfalls of the existing Governance Council in relation to its operation, transparency, and effectiveness, and questioned if it was the appropriate body to govern an expanded NPAS that encompasses WPA.

97. Pelmorex undertook to table a change to the Governance Council's Terms of Reference to formally include up to two WSP representatives, should the Commission require mandatory WSP participation in WPA. Pelmorex also indicated that it currently extends an invitation to the CWTA to attend the Governance Council meetings as an observer.

Commission's analysis and determinations

98. Emergency alerting requires the collaboration of a number of stakeholders, including EMOs, the alert aggregator (Pelmorex), and alert distributors.

99. The Governance Council was established to oversee the operation of the NAAD System specifically, and it does not constitute an overall governance body overseeing the entire NPAS. Modifications to the Governance Council are outside of the scope of this proceeding. Furthermore, the record of the proceeding does not contain sufficient information regarding the establishment of a governance model for a WPA system in Canada.

100. Coordination and co-operation of all involved stakeholders is integral to the effective functioning of a WPA system in the long term, and an effective NPAS more generally. A national forum for emergency alerting, or multi-stakeholder governance model, under the leadership of either Public Safety Canada or SOREM, would be best situated to address ongoing governance issues associated with a WPA system specifically and NPAS more generally.

101. In this decision, the Commission has addressed the issues within its jurisdiction (i.e. the regulation of wireless service providers). In the *Department of Public Safety and Emergency Preparedness Act*, Parliament has mandated the Minister for Public Safety and Emergency Preparedness to ensure coordination across all federal departments and agencies responsible for national security and the safety of Canadians. Public Safety Canada also works with other levels of government, first responders, community groups, and the private sector in relation to emergency management, among other matters.

102. Unless Public Safety Canada establishes a revised governance model, the Governance Council should continue as the coordinating body for the NPAS. The Commission has indicated previously that it may initiate a review of the governance structure of the NAAD System if sufficient evidence is provided to demonstrate that the existing model is ineffective.

103. The Commission acknowledges SOREM's intentions to explore governance mechanisms with other public alerting stakeholders and looks forward to contributing to and seeing the results of its efforts in this regard.

Implementation timeline and monitoring

Implementation timeline

104. In the Notice, Commission sought comments on (i) when it would be appropriate for WSPs to participate in the NPAS, including the timeline for WSPs to implement the technology to enable WPA, and (ii) assuming that WPA is implemented immediately, what percentage of mobile device users could receive emergency alert messages, detailing obstacles in reaching all users, and how this percentage would change over time.

105. EMOs submitted that WPA infrastructure should be implemented immediately. Technology solution providers and WSPs indicated that WPA could be implemented between 3 and 24 months after a decision is issued on mandatory WSP participation in the NPAS. The CWTA and several WSPs submitted that WPA implementation would take at least 12 months after the Commission issues its decision. Freedom Mobile suggested that it could be implemented in 18 months or less. The timelines provided by the WSPs were subject to the use of industry standards.

106. Concerning handset adoption and compatibility, Bell Canada submitted that it already sells six ATIS-compliant devices. One of the devices, the Doro 824, is an accessibility device. Furthermore, two of the devices are available for $0 on a two-year term agreement.

107. Freedom Mobile submitted that 29% of the devices on its network can receive CB alerts, and a further 34% may be able to receive CB alerts.

108. TCC submitted a conservative estimate that within three years, up to 50% of its device base could have WPA-enabled devices, based on current device rollover trends, and assuming a current penetration rate of 0%.

109. Saskatchewan Telecommunications submitted that approximately 95% of its wireless customers may be able to receive WPA if a system is implemented immediately, presuming that all of its customers' devices are CB-compatible, and that the implementation would include both HSPA and LTE networks.

110. Nokia Solutions and Networks Canada Inc. submitted that 100% of new handsets in the United States support wireless emergency alerting services, and that handset vendors are already working on implementing WPA system requirements based on the ATIS standard.

Commission's analysis and determinations

111. There was a general consensus among WSPs represented through the CWTA that implementation of WPA within 12 months after a decision is issued was possible and realistic.

112. The suggestion that WPA could be implemented in as little as three months using LB-SMS was made by Mobilaris and to achieve this timeline, WSPs would have to contract the WPA services from that company. Furthermore, Mobilaris's solution does not currently meet the CLF Guidance. Therefore, it is unrealistic that WPA could be implemented in such a short time frame.

113. Accordingly, a 12-month deadline for the implementation of WPA would be reasonable.

114. In light of the above, the Commission determines that WSPs must implement emergency alert distribution capability on their networks by **6 April 2018**.

115. To receive WPA messages, mobile devices need to conform to the ATIS standard. Although the number of compliant handsets will be low at first, WPA-compatible device penetration should increase rapidly as more compatible devices become available, and as some existing devices are made compatible via software updates.

116. To expedite WPA-compatible device penetration (i.e. the number of devices sold), the Commission sets the following targets for the availability of such devices for sale to subscribers, based on information submitted on the record of the proceeding:

- **within 12 months** of the date of the decision, 50% of devices for sale will need to be WPA-compatible, including at least one handset for $0 and at least one accessible handset; and

- **within 24 months** of the date of the decision, 100% of devices for sale will need to be WPA-compatible, including at least one handset for $0 and at least one accessible handset.

117. As discussed earlier in this decision, there are certain issues relating to WPA implementation that CISC needs to resolve. Therefore, WSPs will not be required to begin distribution of emergency alert messages until the Commission receives CISC's final reports and issues a decision on those matters.

Monitoring

118. The Commission sought comments on what monitoring and compliance measures should be put in place to ensure full WSP participation in WPA.

119. Technology solution provider Comtech submitted that monitoring could be achieved by requiring reporting at different stages of WPA implementation. It submitted that in the pre-deployment phase, the Commission could require all WSPs to report on the testing of their Cell Broadcast Centre to the NAAD System interface to confirm interoperability and functionality of the WPA system. Following implementation, WSPs could report on the results of scheduled test messages.

120. The Government of Manitoba submitted that monitoring of WPA could be similar to what was established for the broadcasting alert system in Broadcasting Regulatory Policy 2014-444.[15]

121. WSPs submitted that monitoring could be carried out through the submission of status reports to the Commission. Bell Canada suggested that the Commission could require WSPs to submit annual reports outlining WPA-compatible device availability and penetration. Eastlink suggested that WSPs could submit a letter confirming that WPA is fully implemented to confirm compliance upon initial

---

[15] Monitoring factors included the general level of industry compliance, transmission effectiveness, alert quality, availability of emergency alert messages to Canadians, as well as the success of system tests and actual emergency alert message distribution.

service implementation only. Eastlink also submitted that as with E9-1-1, ongoing monitoring and compliance mechanisms are not necessary.

122. Halton Region submitted that WSPs could be encouraged to meet WPA obligations through the use of penalties, as appropriate. RCCI also indicated that administrative monetary penalties could be used to address any issues of non-compliance with WPA requirements.

123. MWSI submitted that the Commission could audit WSPs to encourage the procurement and distribution of WPA-enabled mobile devices.

Commission's analysis and determinations

124. In the Commission's view, the best approach to monitoring and ensuring compliance is by setting reporting requirements on WSPs for the implementation of WPA, and where necessary, employing the appropriate regulatory measures to address non-compliance.

125. Accordingly, the Commission **directs** each WSP to file, by **21 May 2018**, and annually thereafter for a period of three years, a report confirming network implementation of alert distribution capability and interoperability with the NAAD System. The report must also contain the results of at least one successful CB test, which must be invisible to end-users, and information on the following:

- LTE network coverage and gaps;
- WPA-compatible device penetration; and
- the number of WPA-compatible devices offered for sale.

Secretary General

Related documents

- *Modern telecommunications services – The path forward for Canada's digital economy*, Telecom Regulatory Policy CRTC 2016-496, 21 December 2016
- *Participation by wireless service providers in the National Public Alerting System*, Telecom Notice of Consultation CRTC 2016-115, 29 March 2016
- *Amendments to various regulations, the standard conditions of licence for video-on-demand undertakings and certain exemption orders – Provisions requiring the mandatory distribution of emergency alert messages*, Broadcasting Regulatory Policy CRTC 2014-444 and Broadcasting Orders CRTC 2014-445, 2014-446, 2014 447 and 2014-448, 29 August 2014
- *The Weather Network/Météomédia – Licence renewal and extension of the mandatory distribution of the service*, Broadcasting Decision CRTC 2011-438, 22 July 2011

- *Mandatory distribution order for The Weather Network and Météomédia*, Broadcasting Order CRTC 2009-340, 11 June 2009, as amended by Broadcasting Orders CRTC 2009-340-1, 24 January 2012; and 2009-340-2, 15 June 2012

- *Conditions of service for wireless competitive local exchange carriers and for emergency services offered by wireless service providers*, Telecom Decision CRTC 2003-53, 12 August 2003, as amended by Telecom Decision CRTC 2003-53-1, 25 September 2003