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

Telecom Decision CRTC 2018-79

PDF version

Ottawa, 23 February 2018

Public record: 8621-C12-01/08

CISC Emergency Services Working Group – Consensus report ESRE0077 regarding cybersecurity best practices for public safety answering points in a Canadian 9-1-1 ecosystem

In anticipation of the transition to next-generation 9-1-1 (NG9-1-1) networks and services in Canada, the Emergency Services Working Group (ESWG) of the CRTC Interconnection Steering Committee (CISC) examined cybersecurity best practices for public safety answering points (PSAPs) interconnecting with current 9-1-1 and future NG9-1-1 networks. The ESWG filed a consensus report with the Commission setting out proposed cybersecurity best practices including the implementation of a clear NG9-1-1 cybersecurity strategy, enhanced cybersecurity policies, and a cybersecurity action plan.

The Commission considers it important for PSAPs to adopt best practices that will benefit Canadians. Having reviewed the ESWG's consensus report, the Commission encourages PSAPs throughout Canada to implement the best practices set out in the ESWG's consensus report.

Background

1. In Canada, when a call to 9-1-1 is made, the call travels from the network on which it was placed (the originating network)[1] to the local specialized 9-1-1 network. The 9-1-1 network determines which 9-1-1 call centre, also known as a public safety answering point (PSAP), serves the area from which the call was placed and directs the call to that PSAP. The appropriate emergency responders, such as fire, police, or ambulance services, are then identified and dispatched as required.
2. Municipal, provincial, and territorial governments are responsible for emergency responders and for the establishment and management of the PSAPs that dispatch them. Internal policies, procedures, and standards for PSAPs and emergency responders are not determined by the Commission, although there exists national collaboration through the Emergency Services Working Group (ESWG)[2] of the CRTC Interconnection Steering Committee (CISC) if the policies, procedures, and standards are directly related to the services provided by telephone service providers (TSPs).

[1] Originating networks include traditional wireline, wireless, and local voice over Internet Protocol (VoIP) telephony networks, as defined in Telecom Regulatory Policy 2016-165.

[2] The ESWG is a working group that deals with technical and operational issues related to 9-1-1 services in Canada.

3. The Commission's jurisdiction is limited to the originating and 9-1-1 networks. The Commission's role, in the 9-1-1 context, is to exercise regulatory oversight over the access provided by TSPs to enable Canadians to contact PSAPs wherever they have been established by the local government. This includes determining national policies, standards, conditions of service, agreements, eligibility to operate, and approval of tariffs for telecommunications services.

4. In Telecom Regulatory Policy 2017-182, the Commission set out its determinations on the implementation and provisioning of next-generation 9-1-1 (NG9-1-1)[3] networks and services in Canada. The Commission, among other things, imposed obligations on NG9-1-1 network providers related to (i) ensuring the reliability, resiliency, and security of NG9-1-1 networks, (ii) reporting on NG9-1-1 outages, and (iii) ensuring privacy in an NG9-1-1 environment.

5. In that decision, the Commission also requested that CISC develop recommendations and guidelines for the implementation of specific industry best practices and standards. These include performance standards and service levels regarding the reliability, resiliency, and security of the NG9-1-1 networks. As noted in that decision, CISC is best positioned to develop such recommendations and guidelines since it is monitoring related National Emergency Number Association (NENA)[4] standards development and lessons learned in other jurisdictions that are implementing NG9-1-1.

6. The Commission did not specifically address the topic of cybersecurity for PSAPs within the Canadian 9-1-1 ecosystem in Telecom Regulatory Policy 2017-182 since PSAPs are not within its jurisdiction.

The ESWG report

7. In anticipation of the transition to NG9-1-1, the ESWG, in September 2015, decided to examine cybersecurity best practices for PSAPs interconnecting with current 9-1-1 and future NG9-1-1 networks. In initiating this task, the ESWG considered that cybersecurity issues could impact the reliability, resiliency, and security of emergency services given the migration to Internet Protocol (IP) networks and with the introduction of real-time NG9-1-1 databases.

---

[3] NG9-1-1 comprises modernized 9-1-1 networks that are based on Internet Protocol (IP), as well as possible new, enhanced, and innovative 9-1-1 services offered over these networks. For example, Canadians could stream video from an emergency incident, send photos of accident damage or a fleeing suspect, or send personal medical information, including accessibility needs, which could greatly aid emergency responders.

[4] NENA works with public policy leaders, emergency services and telecommunications industry partners, public safety associations, and other stakeholder groups to develop and carry out critical programs and initiatives to facilitate the creation of an IP-based NG9-1-1 system and establish industry-leading standards, training, and certifications.

8. On 16 October 2017, the Commission received the following consensus report (the report) from the ESWG:

    - *Cybersecurity Best Practices for PSAPs in a Canadian 9-1-1 Ecosystem*, 14 September 2017 (ESRE0077)

9. The report is based on the views of 9-1-1 stakeholders, including 9-1-1 network providers, PSAPs, and TSPs. It can be found under the "Reports" section of the ESWG page, which is available in the CISC section of the Commission's website at www.crtc.gc.ca.

10. The ESWG filed the report with the Commission for its review and requested that the Commission encourage Canadian PSAPs to consider and implement a number of cybersecurity[5] best practices for PSAPs. The best practices identified in the report consist of a three-step process, as detailed below.

11. Step one involves the development and implementation of a clear 9-1-1 and NG9-1-1 cybersecurity strategy that identifies assets and their owners, including vulnerabilities, threats, and risks to these assets, as well as methods to mitigate them. This strategy can be supported by the use of a number of existing industry-approved reports and recommendations, white papers, tools, and methodologies, as well as the use of common cybersecurity terminology. These cybersecurity strategy standards should be adopted by all PSAPs and should include, but not be limited to, the following:

    - the completion of a self-assessment of current and future capabilities that includes cybersecurity considerations in all new architectures;
    - the selection of an adaptable cybersecurity framework (for example, the latest National Institute of Standards and Technology [NIST] Cybersecurity Framework), and the application of recommended approaches and features to meet goals;
    - the use of basic cybersecurity best practices and a standards-based, non-proprietary approach to facilitate interoperability with NG9-1-1 ESInets[6] and service designs;
    - the creation, promotion, and facilitation of a work and training environment within PSAPs in which cybersecurity awareness and applicable programs are ubiquitous, supplemented by a regular review of security measures, audits, individual refreshers, and follow-ups;

---

[5] The ESWG has adopted the definition of cybersecurity developed by the National Institute of Standards and Technology (NIST). NIST formally defines cybersecurity as "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

[6] Emergency Services IP networks or ESInets are managed IP networks used for emergency communications that can be shared by all public service agencies.

- the establishment of regular assessments of cybersecurity risks and vulnerabilities on ESInet access services, including joint interconnection point risk assessments with neighbouring PSAPs;
- timely notification and information sharing with other PSAPs interconnecting to the same NG9-1-1 network; and
- the inclusion of cybersecurity specifications and requirements, including terms and conditions language for performance, response times, and outage reports in supplier contracts for 9-1-1- and NG9-1-1-related equipment and services.

12. Step two involves the adoption of the additional cybersecurity recommendations that were detailed in a United States Federal Communications Commission (FCC) Task Force on Optimal PSAP Architecture (TFOPA)[7] report. In that report, the TFOPA determined that an additional layer of security, identified as the Emergency Communications Cybersecurity Center (EC3),[8] should be introduced in the future architecture. As stated in its report, the TFOPA has developed a checklist and a detailed roadmap[9] that can be used as a baseline to create a working document for a phased implementation of cybersecurity services in conjunction with the development of any proposed NG9-1-1 systems and services.

13. Step three involves the initiation of a PSAP-appropriate action plan using the cybersecurity strategy and roadmap set out in steps one and two. The ESWG recommended that PSAPs monitor, audit, secure, protect, and report on cybersecurity events that impact NG9-1-1 and ESInet software and hardware functional elements.

Commission's analysis and determinations

14. As noted by the ESWG, the main objective of the report is to promote cybersecurity awareness among various 9-1-1 stakeholders and to secure overall 9-1-1 and NG9-1-1 environments. The Commission notes that PSAPs are not within its jurisdiction and, accordingly, the Commission is not being asked to approve the recommendations in the report. However, the Commission considers it appropriate to review the substantive recommendations in the report, as requested by the ESWG, and to encourage PSAPs to adopt cybersecurity best practices for the benefit of Canadians.

---

[7] The FCC's TFOPA was directed to study and report findings and recommendations on structure and architecture. The TFOPA is a United States federal advisory committee created to provide recommendations to the FCC about what steps PSAPs can take to optimize security, operations, and funding as they migrate to NG9-1-1.

[8] The EC3 model serves to assist and provide guidance to NG9-1-1 stakeholders and ESInet service providers in their design, implementation, and management of credentialing and certificates. This includes the use of best practices; the development of training exercises; the handling of breaches, vulnerabilities, and attacks; and the gathering and sharing of risk information with all authorized stakeholders, including PSAPs.

[9] The checklist and detailed roadmap were developed by the TFOPA based on work previously done by multiple organizations.

15. The Commission considers that there was appropriate stakeholder representation in the development of the ESWG's report pertaining to cybersecurity best practices for PSAPs in a Canadian 9-1-1 ecosystem, and that there was consensus within the ESWG in developing the recommendations in the report.

16. The Commission therefore supports the recommendations made by the ESWG in this regard, noting that the ESWG took into consideration the fact that the NIST Cybersecurity Framework and the TFOPA report are universally supported by emergency service standards development organizations.

17. The EC3 model, identified in the TFOPA report, will assist in determining the required cybersecurity resources in the form of both systems and support personnel to help with the current and future cybersecurity strategy using best practices, the development of training programs, process planning in the event of a cyberattack, as well as the management and sharing of risk information with other PSAPs.

18. Having reviewed the ESWG's report, the Commission encourages Canadian PSAPs to implement the enhanced cybersecurity processes set out in the ESWG report as best practices for current 9-1-1 and NG9-1-1 systems.

19. Further, upon completion of the policy development steps set out in the ESWG report, PSAPs are encouraged to implement appropriate cybersecurity action plans to achieve the desired cybersecurity-specific outcome. The action plans might include steps to monitor, audit, secure, protect, and report on system security, as well as mitigation steps that focus on effective response, system restoration, and resolution in the event of a cyberattack.

20. In summary, the Commission encourages PSAPs throughout Canada to

    - implement a clear NG9-1-1 cybersecurity strategy that identifies assets and their owners, including vulnerabilities, threats, and risks to these assets, as well as how to mitigate them;

    - use the methods and roadmap guidance included in the TFOPA EC3 model to create enhanced cybersecurity policies; and

    - develop a cybersecurity action plan to monitor, audit, secure, protect, and report on cybersecurity events.

Secretary General

Related documents

- *Next-generation 9-1-1 – Modernizing 9-1-1 networks to meet the public safety needs of Canadians*, Telecom Regulatory Policy CRTC 2017-182, 1 June 2017

- *Matters related to the reliability and resiliency of the 9-1-1 networks*, Telecom Regulatory Policy CRTC 2016-165, 2 May 2016