



## Telecom Decision CRTC 2015-432

PDF version

Ottawa, 21 September 2015

*File number: 8621-C12-01/08*

### **CISC Network Working Group – Consensus report on recommendations to deal with telephony denial of service attacks against public safety answering points**

#### **Introduction**

1. Effective access to emergency services is critical to the health and safety of citizens, and is an important part of ensuring that Canadians have access to a world-class communication system.
2. Following incidents reported internationally of telephony denial of service (TDoS) attacks<sup>1</sup> on the administrative telephone lines of public safety answering points (PSAPs),<sup>2</sup> the CRTC Interconnection Steering Committee's (CISC) Emergency Services Working Group (ESWG) proactively requested that the CISC Network Working Group (NTWG) provide recommendations on how to prevent, detect, and stop possible TDoS attacks on PSAPs in Canada. Administrative telephone lines are used for non-emergency purposes, and are not used to receive 9-1-1 calls.
3. On 19 March 2015, the NTWG submitted the following consensus report (the Report) for Commission approval:
  - *Telephony Denial of Service attacks against PSAPs, 5 March 2015 (NTRE054)*
4. The Report can be found under the "Reports" section of the NTWG page, which is available under the CISC section of the Commission's website at [www.crtc.gc.ca](http://www.crtc.gc.ca).

#### **Commission's analysis and determinations**

5. The NTWG's examination of possible TDoS attacks on PSAPs and its recommendations are timely and proactive, since no such attacks have been reported in Canada. Of particular note is the finding that core 9-1-1 networks in Canada are currently protected from possible TDoS attacks, and that there are safeguards and best practices already in place that mitigate risks to 9-1-1 lines.

---

<sup>1</sup> These attacks occur when malicious software is installed on a computer or other device with Internet access. The software uses a voice over Internet Protocol application to flood a telephone line with inbound calls.

<sup>2</sup> PSAPs are 9-1-1 call centres established and managed by provincial/territorial or municipal governments to answer 9-1-1 calls and then dispatch the appropriate emergency responders, i.e. police, fire, or ambulance.

6. Furthermore, the Report's recommended best practices for PSAPs and 9-1-1 network providers<sup>3</sup> would mitigate the risk of TDoS attacks on PSAP administrative lines, and would further enhance the existing safeguards for 9-1-1 lines.
7. As well, the recommended development of new best practices and guidelines for the coordination between PSAPs and telecommunications service providers would provide guidance to PSAPs regarding actions and procedures they could undertake before, during, and after a TDoS attack.
8. The Commission has reviewed and **approves** all recommendations in the Report.
9. Accordingly, the Commission
  - **directs** all 9-1-1 network providers to
    - continue to treat the 10-digit telephone numbers underlying a PSAP's 9-1-1 lines as highly confidential;
    - serve PSAP 9-1-1 and administrative lines from distinct switches;
    - if it is not currently possible to serve PSAP 9-1-1 and administrative lines from distinct switches, avoid using the same telephone number range for both lines; and
    - submit a letter to the Commission, by **8 January 2016**, confirming that they have implemented the above-noted measures and explaining the specific actions they have taken to comply with the Commission's directions.
  - encourages PSAPs to make the changes recommended in the Report in order to protect their ability to prevent 9-1-1 service from being affected by TDoS attacks; and
  - requests that the ESWG
    - develop a document that outlines reporting and escalation procedures for PSAPs, telecommunications service providers, and 9-1-1 network providers in relation to TDoS attacks on PSAPs;
    - prepare a Canadian version of the National Emergency Number Association's Recommended Best Practices Checklist for Denial of Services Attacks Against 9-1-1 Centers; and
    - continue to monitor the issue of TDoS attacks against PSAPs, and inform the Commission of any further industry developments and opportunities for improvement.

Secretary General

---

<sup>3</sup> 9-1-1 network providers supply network access to PSAPs to other carriers and to their own customers when they make a 9-1-1 call. They are incumbent local exchange carriers (ILECs) and small ILECs.