



Cody C
Via FYI.org.nz

17 November 2022

By email

Tēnā koe Cody,

RE: RNZ/Official Information act request - CCTV

I refer to your request for information under the Official Information Act 1982 (OIA) dated 25 October 2022, requesting information in relation to MetService's X509 certificate.

Please find our response to your request below, with the answers provided below each question.

You have the right to seek an investigation and review by the Ombudsman of this decision. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Yours sincerely

Nick Fagerlund
Company Secretary and Legal Counsel



Level 2, 110 Featherston
Street, Wellington 6011



PO Box 722
Wellington 6140



Ph: 04 470 0700
Fax: 04 473 5231



- 1) *Was MetService aware, prior to this request, that you are signing CAP alerts with an expired X509 certificate?*

MetService was not aware that the X509 Certificate used to sign CAP alerts had expired. We would like to thank you for bringing this to our attention. We are currently taking steps to reduce the risk of this reoccurring. MetService has now updated the certificate and reviewed the process for notification and update.

- 2) *Why was MetService issuing CAP alerts using an expired X509 certificate more than 6 months past the expiry? Is there a process to ensure that the CAP signing certificate is renewed on-time? If yes, why did that not happen in this instance?*

The present process for the renewal of the CAP signing certificate is that renewal is actioned after receipt of an annual renewal email or as part of a maintenance release. This is typically sent to the email address of a specific MetService staff member. In this instance this email was sent to an inactive address because the staff member had left MetService. Despite not being ideal, it is not uncommon for organisations to continue operations with an expired certificate for a limited period of time. This process has been reviewed and steps are being taken to reduce the risk of this occurring again.

- 3) *What would have been the potential impact of having an invalid signature on the CAP alert? For example, the alert may have been discarded by a receiver. This may have caused [x] to not evacuate an area. This may have potentially caused loss of life, as an example.*

A certificate is not required as part of the CAP standard and consumers must not reject messages with invalid signatures. MetService has been providing it as a courtesy. MetService's weather warning system continued to operate effectively over the period during which the certificate had been expired. MetService is confident that the expiry created no risk of impacting weather warning services.

Despite the expired certificate, alerts were still being received, processed and displayed as expected in systems external to MetService. The authenticity of the message could still be checked with the expired certificate, if the processing system permitted an expired certificate to be used. Alternatively, processing systems can use CAP alerts without checking or using the digital signature even if included.



Level 2, 110 Featherston
Street, Wellington 6011



PO Box 722
Wellington 6140



Ph: 04 470 0700
Fax: 04 473 5231