

Meeting Date: 12 May 2020

NATIONAL CYBER-SECURITY CENTRE OVERVIEW

SECURITY AND RELIABILITY COUNCIL

Note: This paper has been prepared for the purpose of the Security and Reliability Council (SRC). Content should not be interpreted as representing the views or policy of the Electricity Authority.

1. Cyber-Security specialist presentations and discussion cancelled

- 1.1. The SRC future workplan (at its March meeting) showed the 12 May meeting having cyber-security as its central theme.
- 1.2. One of the key elements of the meeting was to be an industry-driven session where several senior cyber-security specialists from key organisations would attend the meeting and take part in the discussion.
- 1.3. Due to the ongoing pandemic and subsequent restrictions this session has not been possible. This is because of the additional workloads on organisations during the lockdown meant it was not desirable to approach them for this additional task.
- 1.4. In addition to key cyber-security specialists, the Secretariat listed the below action item at the March meeting:

“Secretariat to organise a cyber-security survey to be sent to the participants for review in meeting 31”
- 1.5. For the same reason as above regarding pandemic restrictions and additional workload during the lockdown, the survey was not sent to participants.
- 1.6. Once the business environment returns to normal, the secretariat will organise the survey and present the results to the SRC at a future meeting.

2. National Cyber-Security Centre overview

- 2.1. A key cyber-security specialist is National Cyber Security Centre (NCSC) Engagement Manager. We have arranged for this presentation to continue and it will be the focal point for the shortened cyber-security discussion at the May meeting.
- 2.2. The NCSC is part of the Government Communications Security Bureau. Their role is to help New Zealand's most significant public and private sector organisations to protect their information systems from advanced cyber-borne threats. They work with government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure. Their focus is on detecting and disrupting cyber threats that are typically beyond the capability of commercially available products and service.
- 2.3. Areas of discussion in the presentation should include:
 - a) The challenges facing the sector
 - b) Opportunities for improvement
 - c) How best to obtain assurance about industry vigilance and effectiveness
 - d) Control Systems Security Information Exchange (CSSIE)
- 2.4. The CSSIE is a group run and funded by the NCSC and serves to enable candid exchange of information among trusted industry peers. The group was brought together to provide focus on the critically important control systems found in the bulk-supply side of the electricity industry. As such, the group has had representatives from Transpower, gentailers and distributors.

2. Questions for the SRC to consider

2.1 The SRC may wish to consider the following questions.

- Q1. Does the SRC want to request any particular information from participants in the cyber-security survey?
- Q2. What advice, if any, does the SRC wish to provide to the Authority at this time?