Commonwealth Bank

Commonwealth Bank of Australia
ACN 123 123 124

1 Harbour Street
Sydney NSW 2000

Gary Blair
Executive General Manager

8 April 2013

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899

Dear Ms Honeycutt

Framework to Improve Critical Infrastructure Cyber Security

Thank you for the opportunity to provide a submission to the National Institute of Standards and Technology on the development of a framework to improve critical infrastructure cyber security.

The Commonwealth Bank Group is Australia's largest bank and one of the top 10 banks in the world by market capitalisation. We are a significant part of Australia's banking system and our systems constitute critical infrastructure that underpins the functioning of the Australian economy.

One element of our program to protect ourselves against potential cyber threats is the development a methodology to enhance our understanding firstly, of how an extreme cyber-attack could be orchestrated against an organisation of our stature and secondly, the current and planned state of organisational resilience against that particular style of attack.

This methodology, known as our **Extreme Cyber Scenario Planning Program**, has assisted us in identifying information security control gaps for remediation and has provided assurance as to our readiness to deal with extreme cyber events. Importantly, it has also informed the development of our longer term security strategy.

Our Extreme Cyber Scenario Planning Program has three key components:

- The identification of extreme cyber scenarios through the combined use of Intel's Threat Agent and Risk Assessment (TARA) methodology and an internal risk matrix;
- The development of an attack tree, using Boolean logic, which maps out in detail the steps by which a successful cyber-attack might occur; and
- An assessment of the strength of organisational controls (derived from industry standard control sets), mapped against each component of the attack tree analysis.

Further detail about this methodology is provided in an attachment to this letter. We also presented this methodology at the 2013 RSA Conference[1].

I believe that our Extreme Cyber Scenario Planning Program has the potential to improve organisational cyber resilience, and we are committed to sharing this information with other critical infrastructure organisations with the aim of improving our collective cyber resilience.

I would be happy to provide further detail about our program should you be interested.

Yours sincerely,

Gary Blair
Executive General Manager
Enterprise Privacy, Identity and Cyber
Enterprise Services

[1] https://ae.rsaconference.com/US13/connect/speakerDetail.ww?PERSON_ID=36C04DEBCF27AC55349043E97996F473