Date: 05 April 2013

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

Sub: Developing a Framework to Improve Critical Infrastructure Cybersecurity

*cyberframework@nist.gov*

Currently we are using Australian Department of Defence's "Strategies to mitigate targeted cyber intrusions". According to Defence Signals Directorate (a unit of Australian Department of Defence), "At least 85% of the targeted cyber intrusions that Defence Signals Directorate (DSD) responds to could be prevented by following the first four mitigation strategies listed in our Strategies to Mitigate Targeted Cyber Intrusions". These top 35 mitigation strategies can be found at http://www.dsd.gov.au/publications/Top_35_Mitigations_2012.pdf

Many critical infrastructure providers, private and public organisations in Australia are using this mitigation strategy to improve their cyber security defence mechanisms and we are one among them. One of the driver for the DSD to come-up with this list/strategy is "SANS Top 20 Critical Security Controls". SANS has mapped DSD's top 35 mitigation strategy to SANS top 20 Critical Security Controls. By adopting SANS top 20, we are also implementing recommendations from DSD Top 35.

Implementing these controls forms the basic building blocks of operational security. These are the critical first steps to improve the operational readiness of defending any organisations security posture. We have seen many organisations in Australia adopting either SANS Top 20 or DSD Top 35 in improving their security. Hence including SANS Top 20 security controls in any organisations security risk management framework is a sensible approach. I would highly recommend NIST to incorporate SANS Top 20 Security Controls in developing a framework to improve critical infrastructure cyber security.