

SMART METERS AND NATIONAL SECURITY

Around 2006 Victoria installed very expensive Smart Electricity Meters into all homes in Victoria. The Victorian Auditor General in several reports, described the rollout as a \$2b disaster.

The rest of the Eastern Seaboard is adopting a similar strategy.

These meters are TWO-WAY meters!

- They TRANSMIT data as well as
- RECEIVE data, and
- They can be turned off remotely!

There is absolutely no reason to RECEIVE data! Simpler and cheaper meters can be developed and should be installed.

Neither Digital nor Social CYBER threats can be prevented, and hackers are getting smarter.

Any determined bad actor will eventually penetrate and remotely turn off these utilities at the meter. Only Near Field Connection (NFC) should be allowed.

For NATIONAL SECURITY and as an ANTI-RANSOMWARE measure, it is strongly recommended that the Federal Government MANDATE ONE-WAY TRANSMIT ONLY meters for all devices used for delivery of Electricity, Gas and Water at all households and businesses.

CHEAPER and SAFER, ONE-WAY UTILITY METERS are the only sure protection against a future CYBER ATTACK on our utility infrastructure.

Has the Australian Cyber Security Centre prepared a case to the National Security Committee?

BETTER TO BE SAFE THAN SMART!