I want to start this by congratulating the Australian Commonwealth Government for their commitment to Cyber Security. The difference in government engagement now compared to only five years ago is noteworthy.

The Australian Government is in the difficult position of owning all the negative risk of cyber security whilst not directly owning the ability to defend and improve the security of non-commonwealth government entities. The government has to influence, educate and empower stakeholders which often is a more difficult task than just remediating their systems. However, the Australian Government also operates considerable information security assets that they can, and do, use to help operators of critical infrastructure. I would like to see an increase in the collaboration of Australian government offensive security capabilities (i.e. Cyber Warfare) and Australian Critical Infrastructure Operators. I have just recently completed a hands on and Incident Response (IR) course run by the ACSC in Brisbane and it was an excellent example of the ability of the government to educate and equip cyber defenders.

Specific feedback to relevant questions:

12 - What needs to be done so that cyber security is 'built in' to digital goods and services?

I think a lot of users think this already exists in products when it does not – I think there would be two useful enhancements:

1. **A cyber security rating** - like an energy star rating – that can allow consumers to make better decisions about the cyber security capability of the products and services that they are buying.
2. **Standardised vendor cyber security hardening guides –** to help users and the general public to secure their devices. Vendors should produce cyber security hardening guides that easily explains how to enable security features and to equip users to make informed decisions on the configuration settings of their devices.

16 - How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

The Australian government should partner with Internet Service Providers (ISPs) to build capability and Threat Intelligence Sharing platforms to help ISPs block malicious traffic attacking end users (i.e. DNS blackholing or network blocking)

17 - What changes can Government make to create a hostile environment for malicious cyber actors?

Continue the education workshops it holds with critical infrastructure operators to enable system operators to disrupt and degrade attacker effectiveness.

The Australian Government should consider establishing industry specific Cyber Security Operations Centres (SOC) to assist system operators in rapidly responding to threats. This SOC would have access to logging information from industry operators.

18 - How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

I would like to see better integration of Australian Offensive Cyber Security Capabilities (i.e. Army Cyber Warfare) working with Critical Infrastructure operators. This is called "purple teaming" that is where attack staff (red team) work with defending staff (blue team) to most effectively identify architectural weaknesses, system vulnerabilities and team capability improvement opportunities.

21 - What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

The government should embrace Indicator of Compromise (IOC) automated sharing systems and assist system operators in workshops and configuration advice of how to enable such systems in their environments.