Recommendation #4: Enhanced security checks must be performed, especially on CII systems

- Vulnerability assessments must be conducted regularly.
- Safety reviews, evaluation, and certification of vendor products must be carried out where feasible.
- Penetration testing must be conducted regularly.
- Red teaming should be carried out periodically.
- Threat hunting must be considered.

Recommendation #5: Privileged administrator accounts must be subject to **tighter control and greater monitoring**

- An inventory of administrative accounts should be created to facilitate rationalisation of such accounts.
- All administrators must use two-factor authentication when performing administrative tasks.
- Use of passphrases instead of passwords should be considered to reduce the risk of accounts being compromised.
- Password policies must be implemented and enforced across both domain and local accounts.
- Server local administrator accounts must be centrally managed across the IT network.
- Service accounts with high privileges must be managed and controlled.

Recommendation #6: Incident response processes must be improved for more effective response to cyber attacks

- To ensure that response plans are effective, they must be tested with regular frequency.
- Pre-defined modes of communication must be used during incident response.
- The correct balance must be struck between containment, remediation, and eradication, and the need to monitor an attacker and preserve critical evidence.
- Information and data necessary to investigate an incident must be readily available.
- An Advanced Security Operation Centre or Cyber Defence Centre should be established to improve the ability to detect and respond to intrusions.

Recommendation #7: Partnerships between industry and government to achieve a higher level of collective security

- Threat intelligence sharing should be enhanced.
- Partnerships with Internet Service Providers should be strengthened.
- Defence beyond borders – cross-border and cross-sector partnerships should be strengthened.
- Using a network to defend a network – applying behavioural analytics for collective defence.

Additional 9 Recommendations

Recommendation #8: IT security risk assessments and audit processes must be treated seriously and carried out regularly

- IT security risk assessments and audits are important for ascertaining gaps in an organisation's policies, processes, and procedures.
- IT security risk assessments must be conducted on CII and mission-critical systems annually and upon specified events.
- Audit action items must be remediated.