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.

Recommendation #9: Enhanced safeguards must be put in place to protect electronic medical records

- A clear policy on measures to secure the confidentiality, integrity, and accountability of electronic medical records must be formulated.
- Databases containing patient data must be monitored in real-time for suspicious activity.
- End-user access to the electronic health records should be made more secure.
- Measures should be considered to secure data-at-rest.
- Controls must be put in place to better protect against the risk of data exfiltration.
- Access to sensitive data must be restricted at both the front-end and at the database-level.

Recommendation #10: Domain controllers must be better secured against attack

- The operating system for domain controllers must be more regularly updated to harden these servers against the risk of cyber attack.
- The attack surface for domain controllers should be reduced by limiting login access.
- Administrative access to domain controllers must require two-factor authentication.

Recommendation #11: A robust patch management process must be implemented to address security vulnerabilities

- A clear policy on patch management must be formulated and implemented.
- The patch management process must provide for oversight with the reporting of appropriate metrics.