SEBI's cyber security Framework for KYC registration agencies

November 5, 2019
***Source**: PRS, Monthly Policy Review*

Who are (Know Your Customer) registration agencies?

These are entities registered with the SEBI (under the KYC Registration Agency Regulations, 2011) which maintain KYC records of investors

Why the framework?

SEBI noted that these agencies should have a robust cyber security and resilience framework since they perform an important role of maintaining KYC records of customers in security markets.

About the Framework

Cyber security frameworks include measures and processes intended to prevent cyber-attacks and improve cyber resilience.

Key features of the framework include:

- **Comprehensive policy: KYC registration agencies should formulate a comprehensive cyber security and resilience policy which should include processes to:**
    - Identify critical risks
    - Protect critical assets

- Detect cyber-attacks and
- Respond and recover from such incidents.

- **Governance & chief information security officer: KYC registration agencies should designate a senior official as chief information security officer, who will:**
- Assess, identify and reduce cyber security risks
- Identify appropriate standards and controls, and
- Direct implementation of processes as per the cyber security policy.

- The board of such KYC agencies should constitute a technology committee comprising of experts. This committee will review the implementation of cyber security policy on a quarterly basis.
- **Access control:** Access to registration agencies' systems, applications, databases should be for a defined purpose and a defined period. Physical access to critical systems should be restricted to the minimum and be monitored through controls such as CCTV cameras and card access systems.
- **Sharing of information:** Quarterly reports containing information on cyber-attacks and threats, and measures taken to mitigate vulnerabilities should be submitted to SEBI