**Summary of Recommendations**

RNS recommends the following remedial actions to improve the security hygiene and ensure alignment with best practices to minimize risk exposure.

* Restrict external access by allowing only trusted IPs through firewall rules.
* Disable weak cryptographic algorithms and enforce the use of stronger, more secure alternatives.
* Apply secure SSH configurations to mitigate risks associated with weak key exchanges and cipher usage.
* To disable weak CBC cipher suites, support and enable only ciphers with high encryption.
* Restrict access by closing unnecessary ports and enforcing strict firewall rules.

## **Conclusion and Next Steps**

External Network black box penetration testing uncovered six (6) vulnerabilities potentially leading to confidentiality, integrity and/or availability issues. We recommend remediating these in order of findings severity.

RNS also recommends a periodic black box penetration test as a follow up to this assessment on critical technology assets at the network, layers to uncover more severe findings that may potentially be either exist and/or be introduced in the environment.

**END OF REPORT**