Annexure – I to RFP for IS Audit of RTGS and NEFT related Systems

Baseline Cyber Security Guidelines for NEFT [Part of National Electronic Funds Transfer System Procedural Guidelines Version 1.1 issued by RBI, DPSS]

1. Inventory Management
    - Maintain an up-to-date inventory register of all information assets.
    - Not to use outdated and unsupported hardware or software and monitor software's end-of-support (EOS) date and Annual Maintenance Contract (AMC) dates of IT hardware on an ongoing basis.

2. Prevent installation of unauthorized software: Put in place a mechanism to control installation of software/ applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. In addition, put in place a mechanism to block/ prevent and identify installation and running of unauthorised software/ applications on such devices/ systems.

3. Network Security
    - Use firewalls to protect the network perimeter
    - Ensure perimeter security and block all unnecessary ports
    - Ensure network segmentation to restrict lateral movement of attackers
    - Disable Remote Desktop Protocol (RDP). Restricted access in case of exceptions, may be provided only on need basis through Multi Factor Authentication and with appropriate monitoring.
    - Internet usage is strictly prohibited in SFMS/NEFT/RTGS infrastructure including the zone where these infrastructures are hosted.

4. Change and Patch Management : Ensure robust and documented change management process to assess, approve, implement and review changes made to any technology stack items associated with NEFT systems. Put in place systems and processes to identify, track, manage and monitor the status of patches to all concerned systems (servers, desktops, network devices, operating system and application software).

5. Access Management:

    a. Implement strict user access controls based on principle of least privilege.
    b. Implement multi-factor authentication (MFA) for all critical applications, especially for privileged accounts.

6. Email Security: Implement secure mail and messaging systems that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links, etc. Implement DMARC (Domain based Message Authentication, Reporting & Conformance).

7. Continuous surveillance: Implement mechanism to detect and remedy any unusual activities in critical systems, servers, databases, network devices and endpoints

8. Disaster recovery drills for critical systems should be conducted at least once in a half-year, preferably once a quarter.

9. Backup: Maintain regular and secure backup of critical data and systems, with tested recovery procedures in place.

10. If the entity is providing digital payment products and services to its customers, then ensure compliance to Master Direction on Digital Payment Security Controls related to Internet/ Mobile Banking (refer RBI Circular DoS.CO.CSITE.SEC. No.1852/ 31.01.015/ 2020-21 dated February 18, 2021), as updated from time to time.

11. Application Security Life Cycle (ASLC): Follow a ‘secure by design’ approach in the development of critical applications. Further, ensure that applications are inherently more secure by embedding security within their development lifecycle.

12. Log management: Put in place comprehensive log management procedures addressing aspects of identification of log sources, log generation, log transmission and storage, log normalisation & parsing, log analysis, log disposal, log security and periodic review of log readiness.

13. Conduct Vulnerability Assessment (VA) and Penetration Testing (PT): For critical information systems and/ or those in the De-Militarized Zone (DMZ) having customer interface, VA to be conducted at least once in every six months and PT at least once in 12 months. The risks highlighted to be remediated within defined timelines based on criticality.

14. Cryptographic controls: The key length, algorithms, cipher suites and applicable protocols used in transmission channels, processing of data and authentication purpose shall be strong. Internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable should be adopted, and the configurations involved in implementing such controls shall be compliant with extant laws and regulatory instructions.

15. Members to follow the latest IDRBT CA guidelines related to cryptographic devices and digital certificates. Entities should maintain and operationalize required policy in order to ensure that renewal of Digital Security Certificates (DSCs) are undertaken before expiry of ongoing certificates.

16. Transaction Monitoring: Implement mechanism for identifying suspicious transactional behaviour in respect of rules, preventive, detective types of controls, mechanism to alert the customers in case of failed authentication, time frame for the same, etc.

17. Security Operations Centre(SOC): Set up SOC as provided in Annex-2 of Circular DBS.CO/CSITE/BC 11/33.01.001/2015-16 dated June 02, 2016 on Cyber Security Framework in Banks, as applicable and also factor in DoS.CO/CSITE/BC.4083/31.01.052/2019-20 dated December 31, 2019 on Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach , as applicable.

18. Adherence to rules & guidelines of INFINET, INFINET framework and SFMS, as updated from time to time.

Baseline Cyber Security Guidelines for RTGS [Part of Real Time Gross Settlement System Regulations Version 1.0 issued by RBI, DPSS]

1. Inventory Management:

    - Maintain an up-to-date inventory register of all information assets.
    - Not to use outdated and unsupported hardware or software and monitor software's end-of-support (EOS) date and Annual Maintenance Contract (AMC) dates of IT hardware on an ongoing basis.

2. Prevent installation of unauthorized software: Put in place a mechanism to control installation of software/ applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. In addition, put in place a mechanism to block/ prevent and identify installation and running of unauthorised software/ applications on such devices/ systems.

3. Network Security:

    - Use firewalls to protect the network perimeter
    - Ensure perimeter security and block all unnecessary ports
    - Ensure network segmentation to restrict lateral movement of attackers
    - Disable Remote Desktop Protocol (RDP). Restricted access in case of exceptions, may be provided only on need basis through Multi Factor Authentication and with appropriate monitoring.
    - Internet usage is strictly prohibited in SFMS/NEFT/RTGS infrastructure including the zone where these infrastructures are hosted.

4. Change and Patch Management: Ensure robust and documented change management process to assess, approve, implement and review changes made to any technology stack items associated with RTGS systems. Put in place systems and processes to identify, track, manage and monitor the status of patches to all concerned systems (servers, desktops, network devices, operating system and application software).

5. Access Management:

    - Implement strict user access controls based on principle of least privilege.
    - Implement multi-factor authentication (MFA) for all critical applications, especially for privileged accounts.

6. Email Security: Implement secure mail and messaging systems that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links, etc. Implement DMARC (Domain based Message Authentication, Reporting & Conformance).

7. Continuous surveillance: Implement mechanism to detect and remedy any unusual activities in critical systems, servers, databases, network devices and endpoints.

8. Disaster recovery drills for critical systems should be conducted at least once in a half-year, preferably once a quarter.

9. Backup: Maintain regular and secure backup of critical data and systems, with tested recovery procedures in place.

10. If the entity is providing digital payment products and services to its customers, then ensure compliance to Master Direction on Digital Payment Security Controls related to Internet/ Mobile Banking (refer RBI Circular DoS.CO.CSITE.SEC. No.1852/ 31.01.015/ 2020-21 dated February 18, 2021), as updated from time to time.

11. Application Security Life Cycle (ASLC): Follow a ‘secure by design’ approach in the development of critical applications. Further, ensure that applications are inherently more secure by embedding security within their development lifecycle.

12. Log management: Put in place comprehensive log management procedures addressing aspects of identification of log sources, log generation, log transmission and storage, log normalisation & parsing, log analysis, log disposal, log security and periodic review of log readiness.

13. Conduct Vulnerability Assessment (VA) and Penetration Testing (PT): For critical information systems and/ or those in the De-Militarized Zone (DMZ) having customer interface, VA to be conducted at least once in every six months and PT at least once in 12 months. The risks highlighted to be remediated within defined timelines based on criticality.

14. Cryptographic Controls: The key length, algorithms, cipher suites and applicable protocols used in transmission channels, processing of data and authentication purpose shall be strong. Internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable should be adopted, and the configurations involved in implementing such controls shall be compliant with extant laws and regulatory instructions.

15. Members to follow the latest IDRBT CA guidelines related to cryptographic devices and digital certificates. Entities should maintain and operationalize required policy in order to ensure that renewal of Digital Security Certificates (DSCs) are undertaken before expiry of ongoing certificates.

16. Transaction Monitoring: Implement mechanism for identifying suspicious transactional behaviour in respect of rules, preventive, detective types of controls, mechanism to alert the customers in case of failed authentication, time frame for the same, etc.

17. Security Operations Centre(SOC): Set up SOC as provided in Annex-2 of Circular DBS.CO/CSITE/BC 11/33.01.001/2015-16 dated June 02, 2016 on Cyber Security Framework in Banks, as applicable and also factor in DoS.CO/CSITE/BC.4083/31.01.052/2019-20 dated December 31, 2019 on Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach , as applicable.

18. Adherence to rules & guidelines of INFINET, INFINET framework and SFMS, as updated from time to time.

x-x-x