

STATE BANK OF INDIA – NEW YORK

425 Park Avenue

New York

NY -10022

Date: September 28, 2026

State Bank of India, New York Branch, invites proposals from qualified and experienced firms for Virtual Chief Information Security Officer (vCISO) services for our US Operations, covering New York, Chicago, Los Angeles branches.

Extended last date for submission of proposals: October 30, 2026

The summary details of the RFP are as under:

S. No.	Particulars	Description
1	Detailed Scope of Work	As per Annexure I – Roles and Responsibilities
2	Extended due date for submission of proposals	October 30, 2026
3	Mode and Address for submission of RFP documents	Interested firms can submit their proposals via email to vpsys.nyb@statebank.com or, via physical copies to: Vice President (Systems), State Bank of India, 425 Park Avenue, Floor 33, New York, NY 10022

Disclaimer: This RFP is not an offer by State Bank of India, but an invitation for proposals from potential firms. No contractual obligation whatsoever shall arise from the Request for Proposal process unless and until a formal contract is executed by duly authorized officers of State Bank of India. State Bank of India reserves the right to request submissions or clarifications from one or more firms, or to cancel the process entirely, without assigning any reason thereof. No firm is obligated to respond or to continue responding. State Bank of India reserves the right to alter specifications during the process and (without reissuing the entire RFP) after the selection of a tentative firm. Each party shall be entirely responsible for its own costs and expenses incurred while participating in the RFP response, due diligence, contract negotiation, and proposal preparation processes.

The terms of this Request for Proposal and the information submitted in response hereto shall be deemed confidential information of State Bank of India and shall not be disclosed to any third party without prior written consent from the State Bank of India. If you are required to disclose any confidential information by any legal request, you shall promptly notify State Bank of India in writing prior to responding.

Annexure I: Roles and Responsibilities

Scope of Work

The Virtual Chief Information Security Officer (vCISO) shall be responsible for overseeing, advising, and ensuring implementation of the Bank's Information Security and Cybersecurity program across all U.S. branches — New York, Chicago, and Los Angeles — in compliance with applicable federal and state cybersecurity, data security, and privacy regulations.

- The vCISO engagement shall identify a named lead individual (and a named backup) who will personally serve as CISO for regulatory and reporting purposes; the scope shall not be fulfilled by an unnamed rotating pool of consultants.

Core Roles and Responsibilities for vCISO in US Operations

A. Governance and Regulatory Compliance

- Develop, oversee, and maintain SBI's Cybersecurity Program in compliance with federal and state regulations.
- Enforce SBI's Information Security, Data Security, and Privacy Policies across all U.S. branches and operations.
- Review and update cybersecurity governance frameworks and policies annually to reflect regulatory updates.
- Ensure alignment with GLBA, FFIEC, NIST CSF, ISO 27001, and state privacy mandates (NYDFS, CPRA, PIPA).
- Provide certification of annual compliance with NYDFS 23 NYCRR Part 500, to be reviewed and countersigned by the Country Head – U.S. Operations (or other authorized senior officer of the Bank) prior to filing with NYDFS, as ultimate filing accountability rests with the Bank.
- Advise SBI US OPS senior management on relevant changes in federal or state cybersecurity regulations.

B. Risk Assessment and Security Oversight

- Oversee periodic Vulnerability Assessment and Penetration Testing (VA/PT) across all IT assets and applications.
- Conduct Cybersecurity and Information Security Risk Assessments, ensuring risks are identified, tracked, and mitigated.
- Review and approve Third-Party Risk Assessments for vendors and service providers, including cloud and fintech partners.
- Ensure all branches maintain appropriate technical safeguards—firewalls, endpoint protection, encryption, and secure configuration management.

C. Incident Response and Regulatory Reporting

- Oversee SBI's Cyber Incident Response Plan (CIRP), ensuring readiness and compliance with multi-jurisdictional notification timelines.
- Coordinate incident management and breach notifications in compliance with:
 - o NYDFS Part 500 (Cybersecurity Events)
 - o CCPA/CPRA breach notification requirements
 - o Illinois PIPA breach notification mandates
 - o OCC/FDIC/FRB incident notification rules (36-hour rule for banking organizations)
- The vCISO and designated backup shall be available on a 24x7 basis for incident triage and shall acknowledge notification of a suspected cybersecurity event within two (2) hours, to support the Bank's ability to meet the 36-hour and 72-hour regulatory notification deadlines referenced above.
- Provide post-incident review and recommendations to prevent recurrence.

D. Business Continuity and Cyber Resilience

- Review Business Continuity (BC) and Disaster Recovery (DR) programs for alignment with cybersecurity resilience objectives.
- Ensure regular testing and validation of BC/DR plans with a cyber-incident component.

E. Third-Party and Supply Chain Security

- Review and assess SOC 1/SOC 2 reports and other security certifications of third-party vendors.
- Track remediation of prior audit findings or control gaps in vendor reports.
- Oversee due diligence for critical vendors, ensuring compliance with SBI USOPS Third-Party Risk Management (TPRM) policy.
- Advise on contractual requirements for cybersecurity and data protection across vendor relationships.

F. Data Privacy and Protection

- Oversee compliance with GLBA Safeguards Rule, NYDFS Part 500, CCPA/CPRA, and Illinois PIPA.
- Ensure controls for data classification, encryption, minimization, retention, and disposal are implemented across U.S. branches.
- Coordinate periodic data protection impact assessments (DPIAs).
- Provide guidance on U.S.-specific data subject rights under CPRA and other state laws.

G. Training and Awareness

- Conduct annual cybersecurity and data privacy awareness training for all SBI U.S. Operations employees.

- Promote ongoing awareness initiatives emphasizing phishing prevention, insider threat mitigation, and regulatory responsibilities.

H. Metrics, Audits, and Continuous Improvement

- Monitor Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) for cybersecurity.
- Review internal and external audit reports, regulatory examination findings, and management responses.
- Benchmark SBI's cybersecurity maturity using NIST CSF 2.0 and/or the Cyber Risk Institute (CRI) Profile and NIST CSF.
- Note: the FFIEC Cybersecurity Assessment Tool (CAT) was officially sunset/retired on August 31, 2025, and should not be relied upon as the ongoing benchmarking framework.

I. Strategic and Emerging Threat Advisory

- Provide strategic advice to SBI management on emerging threats.
- Maintain threat intelligence coordination with relevant U.S. and global agencies (FS-ISAC, CISA advisories, etc.).

J. Reporting and Governance Participation

- Participate as a member in SBI's Cybersecurity, IT, and Risk Governance Committees.
- Present quarterly updates on cybersecurity posture, material risks, and incident trends.
- Report significant cybersecurity incidents and program changes to the Country Head – U.S. Operations.
- Provide an annual written report to the Country Head covering:
 - o Overall status and effectiveness of the cybersecurity program.
 - o Compliance with applicable federal and state cybersecurity and privacy regulations.
 - o Material cybersecurity risks and mitigation status.
 - o Summary of incidents and remediation plans.
 - o Recommendations for program improvement.

K. Coordination with Global Information Security Office

- Collaborate with the SBI Group Information Security and Risk Teams to ensure alignment between U.S. operations and global standards.

L. Engagement Governance, Access, and Transition

- The vCISO firm and all assigned personnel shall be bound by a written confidentiality/non-disclosure agreement and shall be subject to background checks commensurate with the level of privileged access granted to the Bank's systems and data.

- Access to the Bank's systems, networks, and sensitive data shall be provisioned under the principle of least privilege, individually attributable, logged, and reviewed periodically by the Bank's designated in-house liaison.
- The vCISO firm shall maintain professional liability (errors & omissions) and cyber liability insurance of a level commensurate with the engagement, evidenced annually to the Bank.
- The vCISO shall provide a minimum defined level of on-site presence at each of the New York, Chicago, and Los Angeles branches (frequency to be specified in the Statement of Work), in addition to virtual coverage.
- In the event the Bank transitions to an in-house/full-time CISO, the vCISO shall provide a documented knowledge-transfer and transition assistance period of no less than 60 days, including handover of the risk register, policy documentation, open remediation items, and vendor/regulator relationships.