



MANILA ELECTRIC COMPANY (MERALCO)
Ortigas Center, Brgy. Ugong, Pasig City

REQUEST FOR INFORMATION

(SCM RFI NO. IP0525-0502-1)

VARIOUS CYBERSECURITY SOLUTIONS

Meralco Cyber Security Group is currently in the process of strengthening Meralco's cybersecurity measures to achieve strengthened cybersecurity defense and incident response capabilities, secure and reliable critical infrastructure, secure and policy-based network access for both users and devices, and enhanced application security posture.

MERALCO invites interested vendors to provide general information and their expertise in any of the following Various Cybersecurity Solutions:

- A. Cybersecurity Analytics Platform** – This security solution is designed to integrate and correlate data across multiple security platforms, providing centralized visibility, automated threat detection, and faster incident response. This platform will unify security operations, improve threat detection and response, and provide a centralized dashboard for reporting, optimizing overall security efficiency.
- B. Security Orchestration, Automation, and Response (SOAR) with Case Management** – This solution aims to centralize, streamline, and automate the organization's incident response operations. This will serve as a comprehensive framework for orchestrating and automating security operations, enabling faster and more effective incident detection, investigation, and response. This platform will support the aggregation and correlation of security events, automate incident response workflows, and streamline case management across the enterprise.
- C. Cybersecurity Integrated Risk Management Platform** – This platform aims to enhance visibility, coordination, and automation across Meralco's enterprise risk landscape. This should unify risk management processes, improve regulatory alignment and decision-making, and provide a centralized dashboard for reporting.
- D. Digital Forensics, Sandboxing, and Dynamic Malware Analysis Tools** – These tools are integral components of cybersecurity used to investigate, understand, and mitigate cyber threats. Through these tools, Meralco aims to detect and understand the nature and impact of cyberattacks; contain and neutralize threats effectively; and collect actionable intelligence and evidence for incident response and legal action.
- E. Cybersecurity Breach and Attack Simulation** – This platform allows proactive testing of defenses by emulating real-world cyberattacks in a controlled environment. This platform will simulate real-world attack scenarios, identify security gaps, and provide actionable insights through a centralized dashboard—enhancing threat detection, response readiness, and overall security effectiveness.
- F. Static Application Security Testing (SAST) Solution** – This solution aims to identify vulnerabilities, insecure coding practices, and potential security flaws before application deployment. This will be integral in strengthening Meralco's software security posture across the development lifecycle, ensuring compliance with industry standards, and supporting secure Development, Security, and Operations (DevSecOps) practices.
- G. Network Access Control (NAC)** – This is a security solution that determines which devices can connect to a network and ensures that these devices meet security requirements. NAC solution provides centralized control to authenticate users and devices, assess their security posture, and enforce network policies. This solution aims to ensure secure and policy-based network access for both users and devices.

Interested vendors may participate to any of the requested RFI above.

CALENDAR OF ACTIVITIES:

ACTIVITY	DATE	TIME
Submission of Letter of Intent	May 09 – 16, 2025	Until 11:59 PM of May 16, 2025
Submission of Non-Disclosure Agreement	May 19 – 26, 2025	Until 11:59 PM of May 26, 2025
Release of RFI documents to Vendors	May 27, 2025	Until 11:59 PM of May 27, 2025

Interested vendors are requested to submit the following:

- Certificate of Authorized Distributorship or Authorized Reseller Certificate (for Local Partners)
- Letter of intent to participate in the Request for Information

Supplemental Information:

- This RFI is non-binding and does not constitute a commitment to acquire vendor's products or services.
- Vendors shall shoulder all costs associated in the preparation of their responses (e.g., preparation of budgetary quotation, conduct of Proof of Concept/ Product Demo, among others).
- Responses received are to be used solely for informational and benchmarking purposes only.
- Documents or information provided with the responses shall become property of MERALCO.
- No bid fees are to be imposed in relation to this RFI.
- Non-Disclosure Agreement (NDA) is required prior the release of RFI document, and confidential data to the vendors.

MERALCO reserves the right to:

- Issue an addendum to the RFI at any time as a result of questions, change in submission schedule, or other matters; and
- To cancel or reissue the RFI on a reasonable basis.

Submission of requested information must be in portable document format (PDF) and must be emailed to **Category Management for ICT - Platform & Cyber Team through their email at group.platform.cyber@meralco.com.ph not later than 11:59 PM, May 16, 2025.** For inquiries or clarifications prior to the submission deadline, vendors may communicate directly to the assigned team.

(sgd.)
GLEN N. SAN PEDRO
Head, Supply Chain Management

MERALCO employs strict cybersecurity controls. Kindly refer to the following link for the Vendor Cybersecurity Advisory: <https://company.meralco.com.ph/news-and-advisories/supply-chain-management-invitations-bid>