



Operations and Logistics Division
Information security and national cyber security
National embezzlement and fraud risk manager
Tel: 076-8642530, Fax: 076-8642576
9/2026



Guiding Questions on Supply Chain Security for Critical Network Products

As part of its procurement activities, the Israel Electric Corporation (IEC) acquires hardware and software products from external suppliers.
IEC requires vendors to demonstrate that appropriate security controls are maintained throughout the product lifecycle, including development, manufacturing, assembly, and delivery.
This document defines the minimum security and supply chain requirements that bidders must meet in order to be considered for further evaluation.
Non-compliance with these requirements may result in disqualification from further participation in the procurement process.

Minimum Secure Development Requirements

To reduce supply chain risk and ensure an adequate level of product security maturity, bidders must comply with the following requirements.

1. Secure Product Development Certification

The manufacturer shall maintain a valid certification to:
IEC 62443-4-1 – Secure Product Development Lifecycle Requirements, issued by an independent and recognized certification body.

Bidders must provide:

- A formal certificate of compliance
- Certification scope
- The legal entity name appearing on the certificate

The procuring organization reserves the right to verify the certification with the issuing body.

The certification must be valid at the time of proposal submission. Commitments to obtain future certification will not be considered compliant.

Failure to provide the required certification may result in disqualification.

2. Applicability of Certification to the Offered Product

The IEC 62443-4-1 certification must apply to the organization responsible for the design, development, and ongoing maintenance of the proposed product.

Where development is performed by an affiliate, subsidiary, OEM partner, or third-party contractor, the certification must cover the actual development entity.

Products based on rebranding, white-label manufacturing, or arrangements in which the bidder does not maintain full control over the secure development lifecycle may be rejected.

3. Product Security Certification – IEC 62443-4-2

The proposed product shall comply with the applicable security requirements of **IEC 62443-4-2 – Security for Industrial Automation and Control Systems – Technical Security Requirements for IACS Components**.

Where applicable, the bidder shall provide evidence that the proposed product has been independently certified to IEC 62443-4-2 by a recognized certification body.

Bidders shall provide:

- IEC 62443-4-2 certificate, where available
- Certification scope and exact product/model covered by the certificate
- Product version and/or firmware version covered by the certification
- Security Level (SL) claimed or certified
- Identification of any exclusions, assumptions, or limitations within the certification scope

Where the proposed product is not independently certified to IEC 62443-4-2, the bidder shall provide a documented gap assessment or compliance statement against the applicable IEC 62443-4-2 requirements.

The procuring organization reserves the right to verify the certification and its applicability to the exact product and software/firmware version being offered.

4. Independent Product Security Testing

The proposed product must undergo independent security evaluation performed by a qualified third party. Bidders shall provide evidence of at least one of the following:

- A recent third-party penetration test
- An independent product security assessment
- Recognized security certification

An executive summary may be submitted in place of the full report.

Failure to demonstrate independent security testing may be considered a material risk in the evaluation.

5. Security Vulnerability Management and Updates

The manufacturer shall maintain an established process for identifying, assessing, and remediating security vulnerabilities throughout the supported lifecycle of the product.

Bidders must confirm that:

- Security vulnerabilities are tracked and risk-assessed in a timely manner
- Security patches or firmware updates are provided when required
- Customers are notified of critical vulnerabilities and available mitigations

The manufacturer shall commit to providing security updates for the duration of the product's supported lifecycle.

Failure to demonstrate an established vulnerability handling process may be considered a material risk.

Strategic Security Hardening Clauses

The procuring organization reserves the right to perform independent security validation of the proposed product, including vulnerability assessments or penetration testing, prior to or following contract award.

The manufacturer shall notify the procuring organization of any critical security vulnerability affecting the proposed product without undue delay and provide remediation guidance.

The manufacturer shall ensure that security support and updates remain available for a minimum period aligned with the declared product support lifecycle.

Software Security

The bidder shall confirm that all software components within the product are controlled, maintained, and protected against unauthorized modification.

Bidders must address the following:

- Whether software and firmware versions are standardized or customer-specific
- The process used to ensure software is up to date and free from known vulnerabilities
- Measures implemented to prevent malware contamination
- Controls protecting access to source code repositories

Hardware Supply Chain Security

Bidders must demonstrate that appropriate controls exist to prevent unauthorized elements from entering production, testing, packaging, and shipping environments.

The response should address:

- Integrity and authenticity of sourced components
- Prevention of counterfeit parts
- Documentation and traceability of component origin
- Ongoing supply chain audits
- Oversight of third-party manufacturers
- Supply chain risk assessment processes
- Protection of sensitive design and manufacturing data
- Incident response related to supply chain threats
- Risk management for international suppliers
- Security awareness among supply chain partners

Shipping and Packaging Security

Bidders shall describe how products are shipped to their destination and protected from tampering, including:

- Packaging responsibility (manufacturer vs. logistics provider)
- Measures ensuring shipment integrity
- Any security adaptations applied to products delivered to Israel

Submission Requirement

Responses must be sufficiently detailed to provide a clear understanding of the bidder's security posture and enable an effective risk evaluation.

Best regards,

Doron Berger

**director of information security and national security cyber
and embezzlement and fraud risk controller**