



1. General Information

To participate in this tender, the bidder is required to provide the following information, which refers generally to the field of cyber defense:

- 1.1. Software Bill of Materials for all components (SBOM).
- 1.2. Hardware Bill of Materials, including chipsets and controllers (HBOM).
- 1.3. Manufacturing, integration and development locations; including where and how the software was compiled, built, and signed; and entities fabricating the PCBs.
- 1.4. Product Lifecycle plan.
- 1.5. A list of all public libraries utilized by the manufacturer during the development of the software or source code, or alternatively a verification and compliance test report issued by a mutually approved third-party entity.
- 1.6. A declaration confirming that all user accounts, access mechanisms, or development-phase utilities utilized during the development process will be fully removed prior to delivery, including but not limited to any backdoor access.
- 1.7. Beneficial Ownership of entities which are involved through subsidiaries or shell companies.

2. Special requirements

The bidder is required to describe its ability to meet the following requirements:

- 2.1. The manufacturer of the product must be ranked, at minimum, among the top five (5) vendors in the Leaders Quadrant of the relevant Gartner Magic Quadrant report, based on the most recent version published as of the final submission date of the proposals.
- 2.2. The bidder must operate in accordance with a documented Software Development Life Cycle (SDLC).
- 2.3. An offer for a product for which fewer than three (3) years remain until its End of Sale (EOS) date, as of the final submission date of the tender proposals, shall not be permitted, in accordance with the manufacturer's official product lifecycle policy.
- 2.4. The bidder undertakes that every product supplied under this tender shall receive support, maintenance, and security updates for a minimum period of five (5) years from the date it is designated as End of Sale (EOS).
- 2.5. Only standard, commercially accepted cryptographic algorithms that are widely implemented and validated in the industry may be used, in accordance with recognized international standards (FIPS 140-3).
- 2.6. Cryptographic keys must be stored in secure hardware and must support rotation.

3. Maintenance

The Bidder shall operate and maintain a permanent technical support center located in Israel (hereinafter: the "Support Center").

The Support Center shall operate a ticketing system that enables documentation, tracking, and reporting of the status of incident handling. The bidder undertakes to assign a qualified professional to handle each incident, according to its severity level and the required area of expertise.

- 3.1. The Support Center must have been continuously operational for at least three (3) years preceding the final submission date of this tender.
- 3.2. The Support Center shall employ, directly or through its permanent employees only, at least two (2) engineers and five (5) technicians, all possessing professional training, proven experience, and relevant technical expertise in the subject matter of this tender.
- 3.3. The Bidder shall, upon IEC's request, provide documentation demonstrating compliance with this section, including details of the personnel, their professional experience, and the operational history of the Support Center.
- 3.4. The Technical Support Center shall operate with full availability for incident handling, in accordance with the service levels (SLA) defined below.
- 3.5. The Support Center shall be available from 9:00 to 17:00, five (5) days a week, for incident handling, as follows:
 - Critical Incident (Severity 1) - significant disruption or complete service outage: maximum response time of 1 hour until service restoration.
 - Major Incident (Severity 2) - substantial degradation of functionality: maximum response time of 5 hours until service restoration.
 - Normal Incident (Severity 3) - maximum response time within the same business day or the following business day.

4. Additional Information Requirements

In order for the system to be ready for future interfacing with cyber-physical critical systems, the bidder is required to provide the following information regarding cyber protection capabilities:

- 4.1. Hot Spot, Wireless NIC or procedure execution via "Run as" feature would be disabled on all components of the system. Radiating devices would be removed from all the components of the system.
- 4.2. All the switches would be managed type and include Port Mirroring.
- 4.3. The system would include 2FA.
- 4.4. All applications, utilities, services, scripts, configuration files, databases, user accounts and all other software not required for the operation of the system would be removed prior to delivery.
- 4.5. Secured access to the configuration of all devices would be made from a dedicated workstation installed at the network. In case portable computer is utilized as a workstation or maintenance station, the portable computer would be dedicated and unique to the system.

- 4.6. Only the final executable files would reside on any part of the system. Source code would be removed prior to delivery.
- 4.7. All components of the system would be capable to self-documenting their activity, in generic format (minimum Syslog). All the events would be generated and stored locally, i.e. be available on the component where the specific event occurred.
- 4.8. The system firmware would be digitally signed. Change of firmware would be allowed by installing a signed version.
- 4.9. The controller would comply with Achilles certifications.