Template RFP for Rogue Device Detection and Zero Trust Hardware Access

A reusable customer-facing procurement template based on the structure of the reference RFP, adapted for Sepio messaging and editable placeholders.

Issued by	Sepio Cyber Systems
Customer / Prospect	[Insert customer organization name]
RFP reference	[Insert RFP number]
Issue date	[Insert issue date]

Template use note: Replace all bracketed placeholders before issuing. This template keeps the original RFP architecture while correcting wording, aligning it to Sepio terminology, and preserving a structured evaluation matrix.

Version: [Insert version]

Table of Contents

1. Background

This section should explain the customer environment, operating footprint, growth plans, and why connected-device risk has become a business and cybersecurity priority.

Customer overview	[Insert organization overview, scale, locations, and operating model]
Strategic context	[Insert business drivers, transformation goals, or modernization initiatives]
Security context	[Insert current cyber-risk context, asset sprawl, or operational blind spots]

2. Problem Statement

Describe the hardware-security or rogue-device problem the organization is trying to solve.

[Insert concise problem statement. Example: Traditional controls that rely on Layer 2-7 telemetry alone cannot reliably identify spoofed, rogue, or supply-chain-compromised hardware devices, creating visibility gaps across endpoints, networks, and distributed operational environments.]

3. Statement of Purpose / Scope

State what the RFP is intended to achieve.

1. Achieve full visibility of connected assets across IT, OT, IoT, and remote environments.

2. Detect and mitigate rogue, spoofed, hidden, or unauthorized hardware devices.

3. Establish a Zero Trust Hardware Access approach grounded in verifiable hardware identity.

4. Improve risk-based policy enforcement and incident response speed.

5. Support compliance, auditability, and executive reporting requirements.

4. Broad Scope of Work

1. Solution deployment and implementation across in-scope endpoints, network infrastructure, and operating environments.

2. Discovery and visibility of managed, unmanaged, and shadow assets.

3. Threat detection and mitigation for rogue devices, malicious peripherals, implants, and spoofed hardware.

4. Policy management and enforcement aligned to business, technical, and risk requirements.

5. Integration with existing security and IT operations platforms.

6. Reporting, dashboards, risk scoring, and compliance outputs.

7. Training, knowledge transfer, and operational readiness support.

8. Ongoing maintenance, updates, SLA-backed support, and account management.

5. Proposed Solution

[Insert customer-specific language describing the desired solution. Sepio-aligned wording example: The organization seeks a rogue device detection and Zero Trust Hardware Access solution that can establish hardware truth, identify devices undetectable by conventional NAC-only approaches, and enable operationally safe response through trafficless visibility, policy automation, and broad security-stack integration.]

6. Terms and Conditions

The bidder shall clearly state its ability to satisfy the requirements defined in this document.

[Customer name] reserves the right to accept or reject any proposal, in whole or in part, at its sole discretion.

Any subcontracting arrangements must be disclosed in the proposal, and the prime bidder remains fully accountable for all deliverables.

The successful bidder shall assign appropriately qualified technical and project personnel and shall not replace key personnel without prior written approval.

All terms and pricing in the submitted proposal shall remain valid for at least [insert number] working days after the submission deadline.

7. Technical Specifications / Scope of Work and Price Schedule

The following sections are intended to be completed by bidders. Additional innovative capabilities may be proposed where they provide clear value.

7.1 Mandatory Eligibility Requirements

#	Preliminary Examination Criteria	Compliance
1	Certificate of incorporation / registration	Pass / Fail
2	Memorandum and Articles of Association or equivalent corporate formation documents	Pass / Fail
3	Valid trading license or equivalent for the current year	Pass / Fail
4	Current tax clearance certificate or equivalent	Pass / Fail
5	Manufacturer authorization letter, where applicable	Pass / Fail
6	Registered power of attorney or equivalent authorization for the signatory	Pass / Fail

7.2 Mandatory Non-Functional Requirements

#	Requirement	Evidence / Details
1	Bidder should be an authorized partner / reseller / implementation provider for the proposed OEM solution.	Proof of partnership or authorization letter
2	Bidder must provide an OEM authorization letter for the proposed offer.	OEM authorization letter
3	Bidder must provide at least two relevant customer references, preferably including one from a financial institution or similarly regulated organization.	Reference list with project summaries
4	Bidder must provide at least two appropriately certified technical resources for	Relevant certifications and CVs

#	Requirement	Evidence / Details
	deployment and support.	

7.3 Mandatory Functional Requirements - Preliminary Remarks

Compliance indication to be used by the bidder: Compliant / Partially Compliant / Not Compliant. A mere "Compliant" response without sufficient explanation, evidence, or cross-reference may receive a lower evaluation score.

Response Type	Meaning
Compliant	Capability is fully provided in the proposed solution and the response includes enough explanation and supporting evidence.
Partially Compliant	Capability is partially provided or requires additional explanation, configuration, or future roadmap.
Not Compliant	Capability is not provided in the proposed solution.

8. Mandatory Requirements

8.1 General Requirements

#	Requirement	Mandatory (Y/N)
1	Bidder must provide direct access or designated customer access to the relevant support / OEM portal where applicable.	Y
2	Solution must include manufacturer-backed 24x7 premium enterprise support or equivalent.	Y
3	Implementation and support must include professional services.	Y
4	Bidder must provide a technical brief document and solution overview.	Y
5	Bidder must submit a high-level technical architecture tailored to the customer environment.	Y
6	Bidder must demonstrate verifiable project management and technical implementation expertise.	Y

8.2 Technical Specifications

1. PHYSICAL LAYER VISIBILITY & HARDWARE IDENTITY

ID	Requirement	Priority	Vendor Response
1	Solution must provide Layer 1 (Physical Layer) visibility independent of network traffic	Mandatory	[Bidder response / section reference]
2	Solution should use hardware fingerprinting / AssetDNA-style identification for unique device identity	Mandatory	[Bidder response / section reference]
3	Detection must be based on device existence and hardware truth, not only on behavior/activity	Mandatory	[Bidder response / section reference]
4	Trafficless monitoring capability (no deep traffic inspection allowed)	Mandatory	[Bidder response / section

ID	Requirement	Priority	Vendor Response
			reference]
5	Ability to validate device identity using electrical / physical characteristics or equivalent hardware-level evidence	Mandatory	[Bidder response / section reference]
6	Ability to detect devices lacking standard identifiers such as IP or MAC addresses	Mandatory	[Bidder response / section reference]
7	Component-level visibility with hardware inventory / HBOM support	Mandatory	[Bidder response / section reference]
8	Detection resilient to spoofing and profile manipulation	Mandatory	[Bidder response / section reference]

2. COMPLETE ASSET VISIBILITY

ID	Requirement	Priority	Vendor Response
9	Discovery of all managed devices across the IT environment	Mandatory	[Bidder response / section reference]
10	Discovery of unmanaged and shadow IT/OT/IoT devices	Mandatory	[Bidder response / section reference]
11	Discovery of hidden devices not visible to conventional security tools	Mandatory	[Bidder response / section reference]
12	Real-time detection and fingerprinting of USB devices (HID, mass storage, composite)	Mandatory	[Bidder response / section reference]
13	Detection of network-connected devices (wired and wireless)	Mandatory	[Bidder response / section reference]
14	Visibility into IT, OT, and IoT assets in a single pane of view	Mandatory	[Bidder response / section reference]
15	Peripheral visibility down to endpoint level	Mandatory	[Bidder response / section reference]
16	Continuous monitoring for idle or passive hardware assets	Mandatory	[Bidder response / section reference]

3. ROGUE DEVICE DETECTION & MITIGATION

ID	Requirement	Priority	Vendor Response
17	Real-time detection of rogue or unauthorized devices	Mandatory	[Bidder response / section reference]
18	Detection of malicious USB devices including BadUSB / Rubber Ducky-style tools	Mandatory	[Bidder response / section reference]
19	Detection of spoofed peripherals impersonating legitimate HID devices	Mandatory	[Bidder response / section reference]
20	Detection of network implants, rogue switches, rogue hubs, taps, and MiTM devices	Mandatory	[Bidder response / section reference]
21	Detection of MAC address spoofing and device impersonation	Mandatory	[Bidder response / section

ID	Requirement	Priority	Vendor Response
			reference]
22	Detection of supply chain compromised hardware and tampered firmware	Mandatory	[Bidder response / section reference]
23	Automatic mitigation or blocking of devices breaching preset rules	Mandatory	[Bidder response / section reference]
24	Actionable remediation guidance with detailed device and connection context	Mandatory	[Bidder response / section reference]

4. USB, WIRELESS, AND ENDPOINT SECURITY

ID	Requirement	Priority	Vendor Response
25	Comprehensive USB security management capabilities	Mandatory	[Bidder response / section reference]
26	Protection against USB-based malware delivery and social-engineering hardware threats	Mandatory	[Bidder response / section reference]
27	Real-time USB interface monitoring and control	Mandatory	[Bidder response / section reference]
28	Detection of MouseJack and wireless mouse / keyboard attacks	Mandatory	[Bidder response / section reference]
29	Identification of vulnerable 2.4 GHz wireless devices and spoofing attempts	Mandatory	[Bidder response / section reference]
30	Protection against wireless HID injection attacks	Preferred	[Bidder response / section reference]

5. ZERO TRUST HARDWARE ACCESS

ID	Requirement	Priority	Vendor Response
31	Zero Trust Hardware Access policy implementation	Mandatory	[Bidder response / section reference]
32	Never trust, always verify approach at the physical layer	Mandatory	[Bidder response / section reference]
33	Hardware-level device identity verification	Mandatory	[Bidder response / section reference]
34	Identity-based access control for hardware devices	Mandatory	[Bidder response / section reference]
35	Support for micro-segmentation and policy orchestration integrations	Mandatory	[Bidder response / section reference]

6. RISK SCORING, POLICY, AND ENFORCEMENT

ID	Requirement	Priority	Vendor Response
36	Automated risk scoring for every connected device	Mandatory	[Bidder response / section

ID	Requirement	Priority	Vendor Response
			reference]
37	Contextual risk scoring based on hardware identity, location, and business context	Mandatory	[Bidder response / section reference]
38	Risk categorization to prioritize remediation	Mandatory	[Bidder response / section reference]
39	Flexible granular policy creation based on business need, device type, vendor, or tags	Mandatory	[Bidder response / section reference]
40	Automated policy enforcement across endpoints and networks	Mandatory	[Bidder response / section reference]
41	Risk-based access control for policy management	Mandatory	[Bidder response / section reference]
42	Predefined policy options that reduce setup time and do not require lengthy baselining	Mandatory	[Bidder response / section reference]

7. INTEGRATION & COMPATIBILITY

ID	Requirement	Priority	Vendor Response
43	Native integrations with major SIEM, SOAR, NAC, EDR/XDR, and directory services	Mandatory	[Bidder response / section reference]
44	Integration with Cisco ISE, ForeScout CounterAct or equivalent NAC platform	Mandatory	[Bidder response / section reference]
45	REST API for custom integrations	Mandatory	[Bidder response / section reference]
46	Support for Windows, macOS, and Linux	Mandatory	[Bidder response / section reference]
47	Support for cloud platform integration such as Microsoft Azure	Preferred	[Bidder response / section reference]

8. COMPLIANCE, REPORTING, AND ANALYTICS

ID	Requirement	Priority	Vendor Response
48	Support for reporting aligned to NIST, PCI-DSS, ISO 27001, and applicable sector regulations	Mandatory	[Bidder response / section reference]
49	Identification of prohibited or banned equipment and supply-chain anomalies	Mandatory	[Bidder response / section reference]
50	Real-time dashboard with complete asset inventory and risk visualization	Mandatory	[Bidder response / section reference]
51	Historical device activity, audit trails, and exportable reports	Mandatory	[Bidder response / section reference]
52	Executive reporting and compliance-gap identification	Mandatory	[Bidder response / section reference]

9. DEPLOYMENT, OPERATIONS, AND SUPPORT

ID	Requirement	Priority	Vendor Response
53	Support for on-premises deployment	Mandatory	[Bidder response / section reference]
54	Support for SaaS or hybrid deployment models	Preferred	[Bidder response / section reference]
55	Lightweight agent option for endpoint monitoring	Mandatory	[Bidder response / section reference]
56	Agentless option where applicable (network)	Mandatory	[Bidder response / section reference]
57	No scanning of network traffic or sensitive data as a prerequisite for detection	Mandatory	[Bidder response / section reference]
58	Scalability for enterprise environments and high availability / failover	Mandatory	[Bidder response / section reference]
59	24-hour initial visibility or similarly rapid time-to-value	Mandatory	[Bidder response / section reference]
60	24x7 technical support, updates, SLA, and training programs	Mandatory	[Bidder response / section reference]

9. Price Schedule

The financial proposal shall list all costs associated with the assignment, including implementation, training, support, subscriptions / licensing, and annual maintenance for the requested term. All applicable taxes must be included unless expressly stated otherwise.

Item	Description of Supplies / Services	Qty	Unit	Unit Price	Total Price
1	[Insert line item description]	[Qty]	[Unit]	[Currency]	[Total]
2	[Insert line item description]	[Qty]	[Unit]	[Currency]	[Total]
3	[Insert line item description]	[Qty]	[Unit]	[Currency]	[Total]
				Subtotal	[Insert]
				Tax	[Insert]
				Grand Total	[Insert]

Pricing currency: [Insert currency requirement]. Any deviations should be clearly stated by the issuer before release.

10. Invitation to Tender

10.1 Preparation of Proposals

A brief description of the firm and relevant experience in similar assignments.

Recent experience on comparable deployments, including project scope, duration, and bidder involvement.

Comments or recommendations regarding the technical specifications.

A methodology describing how the bidder will perform the assignment.

The proposed team structure, responsibilities, and work plan.

The proposed staff by specialization, tasks, and timing.

Any assumptions, dependencies, or customer-provided services required for success.

Documents evidencing eligibility and compliance.

11. Sealing and Marking of Proposals

[Insert customer submission packaging instructions, including whether technical and financial proposals must be separately sealed or uploaded separately.]

12. Validity of Proposals

The bidder's proposal shall remain valid for at least [insert number] working days after the proposal submission deadline.

13. Submission of Proposals

Submission deadline	[Insert date and time]
Submission address / portal	[Insert physical address and/or electronic portal details]
Submission format	[Insert hard-copy / electronic submission requirements]
Questions contact	[Insert procurement contact name / email / phone]

14. Proposal Evaluation and Contract Award

Evaluation may be conducted in three stages: (i) preliminary examination, (ii) detailed technical / commercial evaluation, and (iii) financial comparison.

The contract is not necessarily awarded to the lowest-priced bidder, but to the responsive and responsible bidder offering the best overall value based on the stated evaluation criteria.

The issuer reserves the right to seek clarifications, verify references, and request demonstrations or presentations as part of the evaluation process.

15. Eligibility Criteria

Have legal capacity to enter into a contract.

Not be insolvent, in receivership, bankrupt, or subject to comparable legal proceedings.

Have fulfilled obligations to pay taxes and statutory social contributions.

Not have a disqualifying conflict of interest in relation to this procurement.

Provide all corporate, financial, tax, and authorization documents requested in Section 7.1.

Have been in operation for at least [insert number] years, with a material portion of business related to ICT or cybersecurity services.

16. ESG Requirements

Bidders are expected to demonstrate alignment with environmental, social, and governance principles throughout the duration of the contract.

16.1 Environmental Responsibility

Minimize carbon footprint through efficient technologies and logistics.

Reduce electronic waste and support responsible disposal or recycling.

Avoid hazardous materials and comply with applicable environmental regulations.

16.2 Social Responsibility

Uphold fair labor practices, safe working conditions, and non-discrimination.

Promote diversity, equity, and inclusion.

Demonstrate community engagement or CSR activity where appropriate.

Ensure subcontractors follow similar standards.

16.3 Governance and Ethics

Maintain transparent business practices and comply with anti-corruption, anti-bribery, and data-protection laws.

Disclose conflicts of interest or legal proceedings that could affect performance.

Maintain policies for ethical conduct, whistleblower protection, and responsible sourcing.

16.4 Reporting and Monitoring

The issuer may request documentation demonstrating ESG compliance, including sustainability reports, labor-policy evidence, diversity statistics, or relevant certifications.

17. Technical Proposal Evaluation

Technical proposals may be reviewed for compliance, responsiveness, and quality. Clarifications may be requested where necessary. The issuer should define the evaluation weighting and scoring model before release.

Task	Evaluation Area	Description	Score
B1	Responsiveness to functional requirements	Bidder demonstrates how the proposed solution meets the requested functional requirements and provides clear evidence.	50
B2	Bidder experience	Relevant customer references, preferably including regulated or similarly scaled organizations.	10

Task	Evaluation Area	Description	Score
B3	Skills, certifications, and partner status	Certified engineers, project manager qualifications, and OEM / partner status.	20
B4	Implementation plan and methodology	Timeline, deliverables, accountability matrix, escalation model, testing plan, training, support, and risk mitigation.	10
B5	Solution demonstration	Live demo of threat detection, dashboards, workflows, and operational fit.	5
B6	ESG compliance	Environmental, social, governance, and ethical compliance evidence.	5
	TOTAL		100

Appendix A - Template Administration Checklist

Replace all placeholders in square brackets.

Confirm evaluation weightings, deadlines, and submission details.

Tailor the scope and mandatory requirements to the customer's environment.

Remove any requirements that should be preferred rather than mandatory.

Attach architecture diagrams, response forms, and pricing workbooks if required.