ISAA | Information Systems Agency of Armenia

COMPETITION FOR THE ALLOCATION OF A GRANT

FOR THE IMPLEMENTATION OF A NATIONAL RESEARCH AND DEVELOPMENT PROJECT

FOR A WORKING PROTOTYPE (PROOF-OF-CONCEPT) SOLUTION IN CYBERSECURITY

TECHNICAL TERMS AND CONDITIONS (TOR)

1. Background and Rationale

The Cybersecurity Research and Development (R&D) Grant Program seeks to position Armenia as a regional hub of excellence for cyber innovation, bridging advanced science, applied research, and private-sector commercialization.

Operating under a Public–Private Partnership (PPP) framework and open to national and international consortia, this program enables Armenia to leverage domestic and global expertise while building indigenous capabilities. It funds cutting-edge research in AI-driven cyber defense, a field central to the future of national security and digital economies.

This procurement aims to identify researchers and vendors capable of delivering state-of-the-art cyber-defense innovations. The Grant focuses on the development of scalable, working prototypes and represents a foundational investment in Armenia's ambition to become a leader in mathematically assured, preemptive national cybersecurity.

Armenia has made significant progress in digital transformation and critical infrastructure modernization. However, the accelerating pace of technological change and rising cyber threats have revealed a pressing gap in research, innovation, and advanced cybersecurity capability. Per Gartner:

1. GenAI-enhanced cyberattacks have increased by over 200% year-over-year.

2. Average breach response time has collapsed from nine days (2021) to under one hour (2024), rendering traditional detect-and-respond approaches operationally obsolete.

Rapid digitization of government agencies and private institutions exposes Armenia to billions in potential breach-related losses over the next five years. Current market efforts emphasize operational security and compliance, while the R&D layer, linking research, policy frameworks, and industrial application remains underdeveloped. Without investment in this layer, Armenia risks dependency on foreign technologies and erosion of digital sovereignty.

This Cybersecurity R&D Grant Program addresses this gap by:

- **Establishing a National R&D Platform** to advance frontier cybersecurity technologies and digital trust.
- **Enabling International Collaboration** by inviting world-class institutions, academia, and startups to co-develop solutions in Armenia using mathematically proven formal methods.
- **Strengthening Policy Integration** by aligning research outputs with national cybersecurity strategies and regulatory frameworks.
- **Building a Sustainable Talent Pipeline** through hands-on innovation projects, fellowships, and spin-offs.
- **Promoting Economic Diversification** by nurturing a cyber industry that attracts investment and exports Armenian technologies.

Through these actions, Armenia aims to become a trusted R&D destination capable of delivering globally competitive cybersecurity and secure digital infrastructure solutions.

2. Purpose of the Grant Program

This grant program establishes a national platform for cybersecurity research and innovation, positioning Armenia as a leader in technology-driven solutions.

The initiative specifically funds the development of a working prototype (proof-of-concept). It does not require a full production-grade system. The objective is to validate research approaches, demonstrate technical feasibility, and assess potential policy impact within the defined scope and timeline. The proposals should demonstrate, via a business case, scalability and the pathway to potential full-scale implementation.

The Committee may select up to **two (2) projects** for funding, retaining the right to fund one or none if proposals do not meet strategic, technical, or risk-adjusted evaluation thresholds.

This initiative is not a procurement exercise for operational products; it is a national investment in experimentation, exploration, and working solutions that demonstrate innovative cybersecurity approaches.

3. Strategic Objectives

The program aims to foster frontier-level innovation, empowering vendors to demonstrate solutions that transform cybersecurity defenses. By developing next-generation solutions, Armenia seeks to leapfrog other nations in capability, agility, and assurance.

AI is expected to play a central role in autonomous or semi-autonomous cyber defense systems, advancing policy governance, operational performance, and strategic procurement. AI-driven innovation should target three fundamental advancements:

1. **Enhanced Modeling and Understanding of Cyberattacks** – Predictive insight into threat propagation across complex networks.
2. **Preemptive Security for Remediation and Reasoning** – Identify control gaps and propose corrective actions based on learned attack patterns.
3. **Operational Efficiency Through Automation** – Reduce security operations fatigue by handling routine detection and triage tasks, allowing human experts to focus on strategic challenges.

AI integration is encouraged but not mandatory. Where implemented, strong human-centric guardrails are required, including:

- Human review of AI-generated outputs and remediation steps.
- “Human-in-the-loop” validation for all actions, with no mandatory autonomous remediation.
- Rigorous testing for deterministic, not probabilistic, results.
- Comprehensive logging of AI and human actions.
- Default read-only AI access to prevent unintended modifications.
- Separation of AI from runtime environments to ensure integrity.
- Mathematical assurance of AI decisions via formal methods and verifiable guarantees.

Complementary technologies to enhance AI performance and assurance may include:

- Formal methods for provable correctness of configurations and controls.
- Deterministic models to eliminate randomness in defense actions.
- AI grounding and guard railing to minimize hallucinations or drift.
- Machine learning for anomaly detection, threat intelligence refinement, and signal-to-noise enhancement.
- Cross-layer security modeling across networks, endpoints, cloud, and identity domains.

Solutions combining these approaches will be best positioned to deliver a preemptive, continuous, and mathematically assured cyber defense posture.

4. Scope of Solutions

Proposed solutions should address well-defined environments, including:

- Government digital platforms and e-governance systems
- Critical infrastructure (energy, telecom, transport, finance)

- National data centers or cloud environments
- Sector-specific enterprise environments

Vendors must demonstrate the ability to deliver multi-agency/organization ready prototypes with full PoC validation of scalable, secure, sovereign, and supported operations. Preference will be given to deployment-ready solutions with repeatable, buyer-observed PoCs validated across:

Area	**Capabilities Vendors Are Expected to Demonstrate, Where Applicable to their Proposal**
Scalability & Availability	Elastic, horizontal scaling for multi-agency/organization load; zero-disruption upgrades; automated failover; load balancing
Packaging	Deployable in cloud, on-prem, and air-gapped environments
Multi-Tenancy	Full isolation per agency/partner/organization; RBAC, MFA, least-privilege enforcement; supported across all packaging options
Data Sovereignty	Armenia-resident by default (or as specified)
Product Security	End-to-end encryption (at rest & in transit), mTLS, managed certs, API security, KMS, key rotation, standards-based SDLC (e.g., OWASP SAMM, NIST SSDF)
Compliance	SOC 2, ISO 27001, GDPR (for SaaS)
Disaster Recovery	Tested backups with defined RPO/RTO
DevOps Maturity	CI/CD, observability, incident runbooks, continuous KPI reporting
Enterprise Support	Minimum 8×5 support, roadmap to 24×7; SLAs with explicit ISAA approval

Product Lifecycle	Documented EOL/EOS policies

Advanced Attributes (Mandatory):

Attribute	Description	Expected Outcomes
Complete	Address all known threats and controls	Identify and analyze IOCs and TTPs for maximum defense effectiveness
Preemptive	Close security gaps before exploitation	Detect and remediate gaps in cybersecurity controls proactively
Continuous	Maintain cyber defense posture at all times	Keep configurations updated to prevent attacks by emerging threats
Verifiable	Provide formal, deterministic proof of correctness	All changes to systems are independently verifiable, minimizing false positives/negatives
Comprehensive	Broad applicability across protective devices	Cover leading NGFWs, IDS, IPS, EDRs; roadmap for new device categories acceptable (e.g. Palo Alto, Fortinet, Cisco, etc.)

Techniques to achieve attributes may include:

- Digital twin cyber protective device modeling including threat inspection capabilities
- Formal verification or model checking of protective devices including threat inspection capabilities
- Predictive analytics and AI-driven configuration assurance

- Autonomous policy-governance engines
- High-speed configuration comparison and drift detection
- Multi-vendor abstraction layers
- Advanced scanning, telemetry correlation, or simulation environments

Applicants should demonstrate at least three attributes in their prototype, with a credible pathway to full alignment. Each prototype should represent a clear leap forward in cyber assurance.

Illustrative Use Cases:

1. Multi-Vendor Configuration Baseline Understanding
2. External Attack Surface Management Compliance
3. Policy Analysis for Human Error Prevention
4. Preemptive Cybersecurity Assurance
5. Open Innovation (vendor-defined methods)

Partial capability submissions are acceptable.

Functional Requirements for implementation roadmap:

For each use-case, vendors must provide KPIs demonstrating completeness, preemption, continuity, verifiability, and comprehensiveness. Examples include:

1. Depth of configuration understanding across device types.
2. Measurements based on global policies (e.g., open ports compliance, maximum scanned IPs/ports).
3. Dashboards identifying human errors and remediation status.
4. Periodic updates of known threats covered and uncovered by configurations.

5. Expected Deliverables

Stage 1 – Vendor information gathering of their Research, Design, Technical, Cost and Roadmap Specifications for All Proposed Use Cases:

- Definition and refinement of research problem statement
- Review of scientific, technical, and industry literature
- Development of system architecture, models, or frameworks
- Definition of functional and non-functional requirements
- Identification of assumptions, constraints, limitations
- Preparation of detailed technical design, use-cases and implementation plan
- Roadmap demonstrating timeline, cost planning, ROI, pricing and phased project management
- Please limit responses to no more than 10 pages

Stage 1 concludes with the vendor selection by tender committee.

Stage 2 – Delivery of Prototype Development and Validation:

- Validation of working PoC use-cases
- Delivery of implementation proposal for full-scale solution
- Demonstration of effective governance, coordination, risk management and final success criteria report for each use-case

Timeline:

- Stage 1 vendor selection will occur no later than Q2 2026
- Stage 2 delivery of rapid quarter-by-quarter prototypes to be completed by awarded vendor within 6-9 months of the award

6. Grant Duration and Funding

- **Program Launch:** -

- **Question Period:** -
- **Submission Deadline:** -
- **Maximum Duration per Grant:** 6-9 months from contract signing

Funding Envelope:

- USD 100,000 per R&D use-case per selected vendor
- Co-financing encouraged but not required
- Up to two winners; one or none may be selected

7. Eligible Applicants

Eligible applicants include:

- Private sector organizations (startups, SMEs, established solution providers)
- Consortia combining research and implementation capacity
- Universities, research labs, and academic centers
- Civil society organizations or think tanks

Preference:

- Registered Armenian or Armenian financed companies
- Previous history of operating in Armenia
- Consortia combining local and international partners with complementary expertise

Eligibility Requirements for Roadmap Proposal (five-year plan):

1. **General Requirements:**

- Capability to deliver a functional prototype within 8 months
- Relevant technical or research expertise
- Ability to operate in Armenia directly or via a local partner

- Compliance with Armenian cybersecurity, data, and privacy regulations

2. **Project Vision:**
    - Five-year phased initiative to design, build, and operationalize a national cyber defense system
    - Roadmap with PoC milestones, defined objectives, measurable success criteria, and exit conditions
    - Integration of leading solutions (e.g. NGFW, ZTNA, EDR, Cisco, Fortinet, etc.) and other advanced features for adaptive and resilient cybersecurity
3. **Project Management:**
    - Detailed 5-year plan with engineering tasks, project governance, and risk management
4. **Implementation, License Price and ROI Proposal:**
    - Detailed breakdown tied to milestones and feature delivery
    - Pricing and licensing model
    - Headcount savings with the five-year ROI
    - Selected vendor will negotiate the details and specifics of the five-year plan for successful completion of stage 2
5. **Support & Maintenance:**
    - Scaling to 24×7 in production
6. **Compliance & Security:**
    - Highest standards of regulatory compliance and SDLC adherence
8. **Evaluation Criteria**

Methodology:

- The proposals are evaluated by a committee using weighted scoring
- Process involves two-stage evaluation; only Stage 1 qualifiers proceed to Stage 2

Scoring Scale: 0–5

Score	Description
0	Not addressed/missing
1	Very weak
2	Weak
3	Adequate
4	Strong
5	Excellent

Stage 1 – Vendor information gathering of their Research, Design, Technical, Cost and Roadmap Specifications for All Proposed Use Cases: (0–100 points)

Criterion	Weight	Evaluation Guidance
Relevance to preemptive cyber policy-governance and cyber defense challenge	40%	Alignment with national/sectoral priorities and regulatory frameworks
Innovation & originality	30%	Novelty and originality beyond existing practices
Team capacity & feasibility	30%	Expertise, experience, and ability to deliver within scope and timeframe

Post Stage 2 full five-year roadmap licensing (0–100 points)

Criterion	Weight	Evaluation Guidance

Problem understanding & relevance	15%	Depth of understanding of the identified problem
Technical innovation & methodology	25%	Soundness and rigor of technical/analytical approach
Feasibility & team capability	10%	Readiness, work plan, team composition
Governance, ethics, and responsible data handling	10%	Data protection, ethical considerations, responsible technology use
Future scalability & integration	10%	Potential for scale and integration into frameworks
Budget, ROI & price competitiveness	10%	Clear, justified, cost-effective budget
Strategic alignment & risk-adjusted feasibility	20%	Alignment with national strategy, realistic risk mitigation

High scores are awarded to proposals with clear differentiation, strong public-sector alignment, and credible implementation pathways. Generic or theoretical proposals may receive lower scores even if technically sound.

---

9. Governance and Program Management

- **Contracting Authority:** ISAA
- **Technical Advisory Panel:** Cybersecurity, policy, and digital transformation experts

10. Intellectual Property (IP) and Data

- IP remains with the grantee

- Upon successful completion of stage 2 by the vendor, the government may pursue a five-year contract that includes custom NRE development with a non-exclusive, royalty-free license, OR purchase standard product licenses
- Data privacy, confidentiality and sovereignty must be maintained
- Compliance with Armenian and relevant international regulations

11. Confidentiality

Due to strategic national cyber defense requirements, vendors may submit technical capabilities or support documentation on a confidential basis. Materials must be clearly labeled “Confidential” and submitted in accordance with confidentiality provisions.