COMPETITION FOR THE ALLOCATION OF A

NATIONAL CYBERSECURITY INNOVATION DEMONSTRATION GRANT

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 competition aims to identify researchers and applicants 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.

Unlike traditional research grants that primarily fund early-stage concepts, this Innovation Demonstration Grant seeks to identify, evaluate and accelerate cybersecurity technologies that have already demonstrated an initial level of technical maturity. Applicants are encouraged to present existing working prototypes, demonstrable capabilities, pilot implementations, proof-of-concepts, or other evidence of innovation that can be adapted and matured to address Armenia's strategic cybersecurity priorities. The objective is to reduce technical risk, accelerate adoption, and maximize the impact of public investment.

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 Government may select up to one (1) 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 commercial off-the-shelf products, nor is it intended to fund basic research alone. It is a strategic national innovation program designed to identify, demonstrate, validate and accelerate innovative cybersecurity technologies capable of supporting Armenia's long-term cyber resilience. Preference will be given to solutions that demonstrate measurable technical maturity and a credible pathway toward operational deployment.

---

3. Strategic Objectives

The program aims to foster frontier-level innovation, empowering applicants 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.

Innovation Maturity

To maximize the effectiveness of public investment, ISAA seeks innovative cybersecurity technologies that have progressed beyond theoretical concepts and demonstrate an appropriate level of technical maturity. Evidence may include, but is not limited to, working prototypes, buyer-observed demonstrations, pilot deployments, proof-of-concept implementations, scientific publications, patents, customer references, technology readiness assessments, or other objective evidence of innovation.

Where AI is 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

Applicants shall demonstrate that their proposed R&D solution has progressed beyond the conceptual stage and can be validated through a buyer-observed technical demonstration. Preference will be given to solutions supported by previous proof-of-concept implementations, pilot deployments, early customer adoption, research validation, or other

objective evidence demonstrating technical feasibility and commercialization potential. Evidence may include, but is not limited to, demonstrations conducted for governments, critical infrastructure operators, research institutions, commercial organizations, or equivalent environments.

The following are capability areas applicants are expected to demonstrate in their proposal:

Area	Capabilities Applicants 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, or in air-gapped environments. Prototype solutions may initially be delivered in SaaS or cloud-hosted environments, provided the applicant presents a credible five-year roadmap toward sovereign, on-premises, or air-gapped deployment where required.
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 multiple technology domains and protective devices. At the proof-of-concept stage, support for every product category is not required, provided the applicants demonstrates a credible roadmap for expanded coverage.	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. Innovation (applicant-defined methods)

Partial capability submissions are acceptable.

Functional Requirements for implementation roadmap:

Applicants must provide KPIs demonstrating completeness, preemption, continuity, verifiability, and comprehensiveness. Applicants may propose alternative metrics where these more appropriately demonstrate the intended outcomes. Illustrative 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

The evaluation of proposal shall be conducted through a single accelerated evaluation process comprising the following activities:

Submission Package

Applicants shall submit:

- Technical proposal (maximum ten pages)
- Description of existing prototype
- Solution architecture
- Research and innovation approach
- Five-year commercialization roadmap
- Budget proposal
- Evidence of previous demonstrations

- Evidence of pilot implementations where available
- Customer references where available
- Technical videos (optional)
- Supporting publications, patents or technical papers where applicable

---

Shortlisting

The Evaluation Committee will review all submissions.

ISAA reserves the right to shortlist applicants for technical demonstration.

Technical Demonstration

Shortlisted applicants shall deliver

- Live demonstration
- Technical walkthrough
- Architecture review
- Committee questions
- Innovation assessment
- Future roadmap

Final Selection

Following demonstrations the Evaluation Committee will select one applicant or none.

Funding Envelope:

- The maximum total funding available under this competition is the AMD equivalent of USD 100,000 (one hundred thousand United States dollars), calculated at the official exchange rate of the Central Bank of the Republic of Armenia applicable on the date of contract execution.
- Co-financing and consortium-based applications are encouraged but not required.
- The Evaluation Committee may select one winner or decide not to select any winner.

---

6. 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 but is not limited to
- 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 3-4 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

7. Grounds for Disqualification

The following persons are not eligible to participate in this procedure:

Persons who, as of the date of submission of the Proposal, have been declared bankrupt by a court decision;
Persons who, or whose executive body representative, have within the five years preceding the date of submission of the Proposal been convicted of financing terrorism, offenses involving the exploitation of children or human trafficking, creating or participating in a criminal association, receiving a bribe, giving a bribe, or bribery-related mediation, and offenses against economic activity provided for by law, except in cases where the conviction has been expunged or lifted in accordance with the procedure established by law;
Persons in respect of whom an administrative act establishing liability for anti-competitive agreements, abuse of a dominant position, or unfair competition in the field of procurement has become non-appealable within the three years preceding the date of submission of the Proposal, or, if appealed, has been left unchanged.
Prohibition on Participation of Affiliated Persons.

For the purposes of this clause:

1) Natural persons are deemed interrelated if they are members of the same family, conduct a joint household or joint entrepreneurial activity, or have acted in concert based on common economic interests.

2) A natural person and a legal person are deemed interrelated if they have acted in concert based on common economic interests, or if the natural person or a member of their family is:

a. a participant holding more than ten percent (10%) of the shares of the given legal person;
b. a person able, in a manner not prohibited by RA legislation, to predetermine the decisions of the legal person;
c. the chairman of the board, deputy chairman of the board, a board member, the executive director or their deputy, or the chairman or member of a collegial body performing executive functions of the given legal person;
d. an employee of the legal entity who works under the direct supervision of the executive director or otherwise has material influence over the decision-making of the legal person's governing bodies.

Project Management:

- Detailed 5-year plan with engineering tasks, project governance, and risk management

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 applicant will negotiate the details and specifics of the five-year plan for successful completion of stage 2.

Support & Maintenance:

- Scaling to 24×7 in production

Compliance & Security:

- Highest standards of regulatory compliance and SDLC adherence

---

8. Evaluation Criteria

Methodology:The proposals are evaluated by a committee using weighted scoring

Scoring Scale: 0–5

Score	Description
0	Not addressed/missing
1	Very weak
2	Weak
3	Adequate
4	Strong
5	Excellent
Criterion	Weight
Strategic relevance to Armenian cyber priorities	20%
Innovation and technical differentiation	20%
Technical maturity of existing prototype	20%
Live technical demonstration	20%
Previous PoCs, pilots or early adoption	10%
Team capability and implementation capacity	10%

Evaluation Procedure

- Each Evaluation Committee member shall assign a score from 0 to 5 for each evaluation criterion.
- The final score for each evaluation criterion shall be calculated as the arithmetic average of the scores assigned by all Evaluation Committee members.
- The final weighted score shall be calculated by multiplying the average score for each criterion by its respective weighting.
- The maximum possible total score is 100 points.

The weighted score for each evaluation criterion shall be calculated using the following formula:

Weighted Score = (Score Awarded for the Criterion ÷ 5) × Criterion Weight

Additional Provisions

During the evaluation process, the Evaluation Committee reserves the right to:

- request additional clarifications or supporting documentation;
- require additional live technical demonstrations or presentations;
- verify the accuracy and authenticity of the information submitted by applicants;
- consult independent technical or subject-matter experts;
- amend the evaluation timeline where reasonably justified; and
- negotiate the project scope, milestones, budget, commercial terms, and implementation approach with shortlisted applicants.

Only proposals achieving a minimum total score of 70 out of 100 points shall be eligible for funding consideration.

The final proposal score shall be equal to the sum of the weighted scores awarded for all evaluation criteria. The maximum possible score is 100 points.

The proposal receiving the highest final score shall be selected as the successful proposal.

Generic or purely theoretical proposals may receive lower scores, even where they are technically well-founded.

Solutions incorporating artificial intelligence shall be sufficiently transparent to permit independent technical evaluation by the Evaluation Committee. Upon request, applicants shall provide access to the underlying implementation through source code walkthroughs, model documentation, algorithms, training and validation methodologies, datasets (where legally permissible), model evaluation results, and other technical artefacts necessary to verify the scientific basis, correctness, robustness, and effectiveness of the proposed solution. Black-box demonstrations without sufficient technical transparency may be deemed insufficient for evaluation.

9. Proposal submission procedure

Applicants shall submit their proposals by:

- Email

Proposals and all documents required under this Call shall be submitted electronically to **procurement@isaa.am** no later than **11:00 AM (Yerevan time) on 2 September 2026.**

All documents shall be submitted in PDF format. The subject line of the email shall state:

Proposal for the Provision of Services

During the evaluation process, the Foundation may request the original copies of the submitted documents for verification.

An applicant may not submit more than one Proposal under this competition. If an applicant submits more than one Proposal, all Proposals submitted by that applicant shall be deemed invalid and shall not be considered by the Foundation.

The Proposal and supporting documents shall include:

Annex 2

Proposal Submission Form

Required Information	Details
Name of the Applicant Organization	
State Registration Number	
Registered Business Address	
Mobile Telephone Number	
Tax Identification Number (TIN)	
Full Name of the Authorized Signatory	
Passport or National ID Card Details of the Authorized Signatory	
Position of the Authorized Signatory within the Applicant Organization	
Date of Proposal Submission	
Signature of the Authorized Signatory	
Total Proposed Price for the Services (AMD, inclusive of all applicable taxes)	

The applicant shall submit the following supporting documentation together with the Proposal:

- Technical Proposal (maximum 10 pages);
- Description of the existing prototype;
- Solution Architecture;

- Description of the research and innovation approach;
- Five-year Commercialization Roadmap;
- Evidence of previous technical demonstrations;
- Evidence of previous Pilot Implementations (where available);
- Customer references (where available);
- Technical demonstration videos (optional);
- Scientific publications, patents, or technical papers (where available);
- Documentation demonstrating previous Proofs of Concept (PoCs), pilot projects, or evidence of early adoption;
- Information on the proposed project team, including CVs of key personnel and evidence of relevant professional experience.

Failure to submit the mandatory supporting documentation required under this Call, or submission of insufficient supporting documentation, shall constitute grounds for rejection of the Proposal.

The Proposal and all supporting documentation may be submitted in Armenian or English.

---

10. Intellectual Property (IP) and Data

- IP, including all pre-existing intellectual property and proprietary technologies of the grantee, remains with the grantee.
- Upon completion of the evaluation process and successful execution of the Innovation Demonstration Grant, the Government may negotiate a subsequent implementation, commercialization, or long-term partnership agreement, including but not limited to non-recurring engineering (NRE), custom development, licensing, or operational deployment arrangements.

- Data privacy, confidentiality and sovereignty must be maintained
- Compliance with Armenian and relevant international regulations

---

11. Opening, Evaluation, and Summary of Results

The deadline for submission of Proposals is 11:00 AM on 2 September 2026. The opening of Proposals shall take place at the address Vazgen Sargsyan 26/1, Office 400, on 2 September 2026 at 11:00 AM. Questions seeking clarification regarding this Invitation may be submitted no later than 18:00 on 25 August 2026 to the email address procurement@isaa.am.

The Foundation's procurement specialist shall prepare a summary report on the Proposals received.

Proposals submitted shall be reviewed and summarized on the basis of the report described in Clause 5.1 at the Committee's meeting for reviewing and summarizing Proposals, to be held no later than 10 September 2026.

Within two (2) business days following the conclusion of the review and summary meeting, the Evaluation Committee shall prepare a protocol regarding the results of the Proposals, which shall include:

The location, date, and time of the opening and summarizing of Proposals, as well as the names, surnames, and positions of the Evaluation Committee members and any invited specialists participating in the meeting;
Information regarding the Proposals submitted;
The name/title of the winner of the competition;
The criteria on the basis of which one of the competition participants was declared the winner;
Any other necessary information.

12. Declaring the Procedure Void

The competition shall be deemed void if:

No Proposal has been submitted to the competition;
All submitted Proposals fail to meet the requirements set forth in this Invitation;
The Evaluation Committee has failed to determine a winner due to non-compliance of Proposals or the results of the evaluation;
The winner of the competition has declined to enter into the contract, and no new winner has been declared in accordance with the procedure set forth in Clause 6.2 of this Invitation;
Participants have failed to comply with other mandatory requirements set forth in this Invitation.

In the cases provided for under this clause, the Contracting Authority shall have the right to declare the competition void without any liability or compensation to participants.

In the event that false, distorted, or misleading information is submitted, the Foundation shall have the right to reject the participant's Proposal at any stage.

---

13. Confidentiality

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