Պատվիրատու՝ Հայաստանի Տեղեկատվական Համակարգերի Գործակալություն
Հիմնադրամ

Հայտարարության սույն տեքստը հաստատված է գնման հանձնաժողովի

2026-08-07-ի N 1 որոշմամբ

Ընթացակարգի ծածկագիրը՝ ՀՏՀԳ-ԲՄԾՁԲ-26-2

ՀՐԱՎԵՐ

«Կիբեռանվտանգության ոլորտում աշխատող նախատիպային (Proof of Concept – PoC) լուծումների մշակման համար ազգային կիբեռանվտանգության նորարարական ցուցադրական դրամաշնորհի մրցույթի»

Հարգելի՛ մասնակից, նախքան հայտ կազմելը և ներկայացնելը խնդրում ենք մանրամասնորեն ուսումնասիրել սույն հրավերը, քանի որ հրավերի բովանդակությանը չհամապատասխանող հայտերը ենթակա են մերժման:

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

Սույն հրավերը նպատակ ունի «Հայաստանի Տեղեկատվական Համակարգերի Գործակալություն» Հիմնադրամի (այսուհետ նաև՝ ՀՏՀԳ կամ Պատվիրատու) կողմից հայտարարված դրամաշնորհի մրցույթին մասնակցելու մտադրություն ունեցող անձանց (այսուհետ նաև՝ Մասնակից) տեղեկացնելու պայմանների, գնման առարկայի, ընտրված առաջարկի որոշելուև հիմնական դրույթների մասին: Հայտեր կարող են ներկայացնել գրանցված իրավաբանական անձինք: Սույն ընթացակարգի հետ կապված հարաբերությունների նկատմամբ կիրառվում է ՀՀ օրենսդրությունը: Սույն ընթացակարգի հետ կապված վեճերը ենթակա են քննության ՀՀ դատավարական իրավունքի նորմերի ներքո:

Մրցութային հանձնաժողովի կոնտակտային անձ՝ Արփինե Կարապետյան (էլեկտրոնային փոստ՝ arpine.karapetyan@isaa.am հեռ. +374 98173434):

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

ՄԱՍ 1

1. ԳՆՄԱՆ ԱՌԱՐԿԱՅԻ ԲՆՈՒԹԱԳԻՐ

«Կիբեռանվտանգության ոլորտում աշխատող նախատիպային (Proof of Concept – PoC) լուծումների մշակման համար ազգային կիբեռանվտանգության նորարարական ցուցադրական դրամաշնորհի մրցույթ»

Տեխնիկական առաջադրանքը կցվում է հայերեն և անգլերեն լեզուներով, անհամապատասխանությունների դեպքում հիմք է ընդունվում հայերեն տարբերակը:

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

ՄԱՍ 1

1. ԲՆՈՒԹԱԳԻՐ ԵՎ ՀԻՄՆԱԿԱՆ ԴՐՈՒՅԹՆԵՐ

Նախապատմություն և հիմնավորում

Կիբեռանվտանգության հետազոտությունների և զարգացման (R&D) դրամաշնորհային ծրագիրը նպատակ ունի Հայաստանը դիրքավորել որպես կիբեռանվտանգության նորարարությունների տարածաշրջանային առաջատար կենտրոն՝ միավորելով առաջատար գիտությունը, կիրառական հետազոտությունները և մասնավոր հատվածի առևտրայնացման հնարավորությունները:

Գործելով պետական և մասնավոր հատվածների համագործակցության (Public–Private Partnership, PPP) շրջանակում և բաց լինելով ինչպես ազգային, այնպես էլ միջազգային կոնսորցիումների համար՝ ծրագիրը հնարավորություն է տալիս Հայաստանին օգտագործել տեղական և միջազգային փորձը՝ միաժամանակ զարգացնելով սեփական ազգային կարողությունները: Ծրագիրը ֆինանսավորում է արհեստական բանականությամբ (AI) պայմանավորված կիբեռպաշտպանության ոլորտի առաջատար հետազոտություններ, որոնք առանցքային նշանակություն ունեն ազգային անվտանգության և թվային տնտեսությունների ապագայի համար:

Այս մրցույթի նպատակն է բացահայտել հետազոտողներին և դիմորդներին, որոնք ունակ են մշակելու և ներկայացնելու կիբեռպաշտպանության ոլորտի ժամանակակից նորարարական լուծումներ: Դրամաշնորհը կենտրոնացած է մասշտաբավորվող և աշխատունակ նախատիպերի (Working Prototype) մշակման վրա և հանդիսանում է Հայաստանի՝ մաթեմատիկորեն հիմնավորված և կանխարգելիչ ազգային կիբեռանվտանգության ոլորտում առաջատար դառնալու ռազմավարական տեսլականի հիմնարար ներդրում:

Ի տարբերություն ավանդական հետազոտական դրամաշնորհների, որոնք հիմնականում ֆինանսավորում են վաղ փուլում գտնվող գաղափարները, այս Նորարարության ցուցադրական դրամաշնորհը (Innovation Demonstration Grant) նպատակ ունի բացահայտել, գնահատել և արագացնել այն կիբեռանվտանգության տեխնոլոգիաների զարգացումը, որոնք արդեն իսկ ցուցադրել են տեխնիկական հասունության որոշակի մակարդակ: Դիմորդներին խրախուսվում է ներկայացնել

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

առկա աշխատունակ նախատիպեր, ցուցադրելի հնարավորություններ, փորձնական ներդրումներ (Pilot Implementations), հայեցակարգի ապացույցներ (Proof of Concept) կամ նորարարության այլ ապացույցներ, որոնք հնարավոր է կատարելագործել և հարմարեցնել՝ Հայաստանի ռազմավարական կիբեռանվտանգության առաջնահերթություններին համապատասխանեցնելու նպատակով: Ծրագրի հիմնական նպատակն է նվազեցնել տեխնիկական ռիսկերը, արագացնել լուծումների կիրառումը և առավելագույնի հասցնել պետական ներդրումների արդյունավետությունը:

Հայաստանը վերջին տարիներին զգալի առաջընթաց է գրանցել թվային վերափոխման և կարևոր ենթակառուցվածքների արդիականացման ուղղությամբ: Սակայն տեխնոլոգիական արագ զարգացումը և աճող կիբեռսպառնալիքները բացահայտել են հետազոտությունների, նորարարության և առաջադեմ կիբեռանվտանգային կարողությունների զարգացման զգալի բացեր: Gartner-ի տվյալներով՝

- Գեներատիվ արհեստական բանականությամբ (GenAI) ուժեղացված կիբեռհարձակումների թիվը տարեցտարի աճել է ավելի քան 200%-ով:
- Անվտանգության խախտումներին արձագանքելու միջին ժամանակը 2021 թվականի 9 օրից 2024 թվականին կրճատվել է մինչև մեկ ժամից պակաս, ինչի հետևանքով ավանդական «հայտնաբերել և արձագանքել» (detect-and-respond) մոտեցումները գործնականում կորցնում են իրենց արդյունավետությունը:

Պետական մարմինների և մասնավոր կազմակերպությունների արագ թվայնացումը առաջիկա հինգ տարիների ընթացքում Հայաստանը ենթարկում է կիբեռանվտանգության խախտումների հետևանքով միլիարդավոր դոլարների հնարավոր վնասների ռիսկին: Այսօր շուկան հիմնականում կենտրոնացած է օպերացիոն անվտանգության և համապատասխանության ապահովման վրա, մինչդեռ հետազոտության և զարգացման (R&D) այն շերտը, որը կապում է գիտական հետազոտությունները, պետական քաղաքականությունը և արդյունաբերական կիրառությունը, շարունակում է մնալ թերզարգացած: Առանց այդ ուղղությամբ

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

ներդրումների Հայաստանը կարող է ավելի մեծ կախվածություն ունենալ արտասահմանյան տեխնոլոգիաներից և կորցնել իր թվային ինքնիշխանությունը:

Կիբեռանվտանգության հետազոտությունների և զարգացման այս դրամաշնորհային ծրագիրը նպատակ ունի հաղթահարել նշված մարտահրավերները՝

- ստեղծելով ազգային R&D հարթակ՝ կիբեռանվտանգության առաջատար տեխնոլոգիաների և թվային վստահության զարգացման համար,
- խթանելով միջազգային համագործակցությունը՝ ներգրավելով համաշխարհային առաջատար հաստատություններին, ակադեմիական շրջանակներին և ստարտափներին՝ Հայաստանում համատեղ լուծումներ մշակելու նպատակով՝ մաթեմատիկորեն ապացուցված ձևական մեթոդների (Formal Methods) կիրառմամբ,
- ապահովելով հետազոտությունների արդյունքների համապատասխանեցումը ազգային կիբեռանվտանգության ռազմավարություններին և կարգավորող շրջանակներին,
- ձևավորելով կայուն մասնագիտական ներուժ՝ նորարարական նախագծերի, կրթաթոշակների և սպին-օֆֆ նախաձեռնությունների միջոցով,
- նպաստելով տնտեսության դիվերսիֆիկացմանը՝ զարգացնելով կիբեռանվտանգության ոլորտը, ներգրավելով ներդրումներ և խթանելով հայկական տեխնոլոգիաների արտահանումը:

Այս քայլերի միջոցով Հայաստանը նպատակ ունի դառնալ վստահելի հետազոտությունների և զարգացման կենտրոն, որն ունակ կլինի մշակել միջազգային մակարդակով մրցունակ կիբեռանվտանգային և անվտանգ թվային ենթակառուցվածքային լուծումներ:

Ռազմավարական նպատակներ

Ծրագիրը նպատակ ունի խթանել առաջատար մակարդակի նորարարությունները՝ հնարավորություն տալով դիմորդներին ներկայացնել այնպիսի լուծումներ, որոնք կարող են էապես փոխակերպել կիբեռանվտանգության պաշտպանության համակարգերը: Մշակելով հաջորդ սերնդի լուծումներ՝ Հայաստանը նպատակ ունի

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

ապահովել զգալի առաջընթաց՝ գերազանցելով այլ երկրների հնարավորությունները, ճկունությունը և անվտանգության ապահովման մակարդակը:

Ակնկալվում է, որ արհեստական բանականությունը (AI) առանցքային դեր կխաղա ինքնավար կամ կիսաինքնավար կիբեռպաշտպանության համակարգերում՝ նպաստելով քաղաքականության կառավարմանը, գործառնական արդյունավետության բարձրացմանը և ռազմավարական որոշումների կայացմանը: AI-ի կիրառմամբ նորարարական լուծումները պետք է ուղղված լինեն հետևյալ երեք հիմնական առաջընթացներին.

- **Կիբեռհարձակումների ընդլայնված մոդելավորում և վերլուծություն** – ապահովել կանխատեսողական պատկերացում բարդ ցանցերում սպառնալիքների տարածման վերաբերյալ:
- **Կանխարգելիչ անվտանգություն՝ շտկման և վերլուծական որոշումների համար** – բացահայտել անվտանգության վերահսկողության թերությունները և առաջարկել համապատասխան ուղղիչ միջոցառումներ՝ հիմնվելով նախկին հարձակումների օրինաչափությունների վրա:
- **Գործառնական արդյունավետության բարձրացում ավտոմատացման միջոցով** – նվազեցնել անվտանգության գործառնական թիմերի ծանրաբեռնվածությունը՝ ավտոմատացնելով սովորական հայտնաբերման և նախնական վերլուծության (triage) գործընթացները, որպեսզի մասնագետները կարողանան կենտրոնանալ առավել ռազմավարական խնդիրների վրա:

Արհեստական բանականության ինտեգրումը խրախուսվում է, սակայն պարտադիր պահանջ չէ:

Նորարարության տեխնիկական հասունություն

Պետական ներդրումների արդյունավետությունն առավելագույնի հասցնելու նպատակով ՀՏՀԳ-ն հետաքրքրված է այնպիսի նորարարական կիբեռանվտանգության տեխնոլոգիաներով, որոնք արդեն անցել են տեսական գաղափարի փուլը և ցուցադրում են տեխնիկական հասունության բավարար մակարդակ: Դրա ապացույց կարող են հանդիսանալ, մասնավորապես, աշխատունակ նախատիպերը, պատվիրատուի կողմից դիտարկված տեխնիկական

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

ցուցադրությունները, փորձնական ներդրումները (pilot deployments), Proof of Concept-ները, գիտական հրապարակումները, արտոնագրերը, հաճախորդների երաշխավորագրերը, տեխնոլոգիական պատրաստվածության գնահատումները կամ նորարարությունը հիմնավորող այլ օբյեկտիվ ապացույցներ:

Այն դեպքերում, երբ լուծումը ներառում է արհեստական բանականություն, պարտադիր է ապահովել մարդու վերահսկողության արդյունավետ մեխանիզմներ, այդ թվում՝

- AI-ի կողմից գեներացված արդյունքների և առաջարկվող ուղղիչ գործողությունների մարդու կողմից վերանայում,
- «Human-in-the-loop» սկզբունքով բոլոր գործողությունների հաստատում՝ բացառելով պարտադիր ինքնավար շտկումները,
- խիստ փորձարկումներ՝ դետերմինիստական, այլ ոչ հավանականային արդյունքներ ապահովելու նպատակով,
- AI-ի և մարդու բոլոր գործողությունների ամբողջական գրանցում,
- AI-ի համար միայն ընթերցման (read-only) հասանելիության ապահովում՝ չնախատեսված փոփոխությունները կանխելու նպատակով,
- AI բաղադրիչի տարանջատում գործառնական միջավայրից՝ համակարգի ամբողջականությունն ապահովելու համար,
- AI-ի որոշումների մաթեմատիկական հիմնավորվածության ապահովում՝ ձևական մեթոդների (Formal Methods) և ստուգելի երաշխիքների կիրառմամբ:

AI-ի արդյունավետությունն ու հուսալիությունը բարձրացնելու նպատակով կարող են կիրառվել նաև հետևյալ լրացուցիչ տեխնոլոգիաները.

- ձևական մեթոդներ՝ կարգավորումների և անվտանգության վերահսկողությունների ճշգրտությունը ապացուցելու համար,
- դետերմինիստական մոդելներ՝ պաշտպանական գործողություններից պատահականությունը բացառելու նպատակով,

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

- AI-ի grounding և guardrailing մեխանիզմներ՝ հալյուցինացիաների և շեղումների հավանականությունը նվազեցնելու համար,
- մեքենայական ուսուցում՝ անոմալիաների հայտնաբերման, սպառնալիքների հետախուզական տվյալների կատարելագործման և ազդանշան/աղմուկ հարաբերակցության բարելավման նպատակով,
- ցանցերի, վերջնակետերի (endpoints), ամպային (cloud) և ինքնության կառավարման (identity) համակարգերի միջև բազմաշերտ անվտանգության մոդելավորում:

Այս մոտեցումների համադրությամբ մշակված լուծումները լավագույնս կկարողանան ապահովել կանխարգելիչ, շարունակական և մաթեմատիկորեն հիմնավորված կիբեռպաշտպանության համակարգ:

Լուծումների շրջանակը

Առաջարկվող լուծումները պետք է նախատեսված լինեն հստակ սահմանված կիրառման միջավայրերի համար, այդ թվում՝

- պետական թվային հարթակներ և էլեկտրոնային կառավարման համակարգեր,
- կարևոր ենթակառուցվածքներ (էներգետիկա, հեռահաղորդակցություն, տրանսպորտ, ֆինանսական համակարգ),
- ազգային տվյալների մշակման կենտրոններ կամ ամպային (cloud) միջավայրեր,
- ոլորտային ձեռնարկությունների տեղեկատվական միջավայրեր:

Դիմորդները պետք է հիմնավորեն, որ իրենց առաջարկվող լուծումն արդեն հաղթահարել է գաղափարային փուլը և կարող է հաստատվել պատվիրատուի կողմից դիտարկվող տեխնիկական ցուցադրության միջոցով: Նախապատվությունը կտրվի այն լուծումներին, որոնք հիմնված են նախկինում իրականացված Proof of Concept-ների, փորձնական ներդրումների (Pilot Deployments), վաղ փուլում հաճախորդների կողմից կիրառման, հետազոտական արդյունքների կամ տեխնիկական իրագործելիությունն ու առևտրայնացման ներուժը հաստատող այլ օբյեկտիվ ապացույցների վրա: Այդպիսի ապացույցներ կարող են լինել պետական մարմինների,

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

կարևոր ենթակառուցվածքների օպերատորների, գիտահետազոտական հաստատությունների, առևտրային կազմակերպությունների կամ համարժեք այլ միջավայրերի համար իրականացված ցուցադրությունները:

Դիմորդները, ըստ իրենց առաջարկի կիրառելիության, պետք է ներկայացնեն հետևյալ կարողությունները.

Ոլորտ	**Պահանջվող կարողություններ**
Մասշտաբայնություն և հասանելիություն (Scalability & Availability)	Էլաստիկ հորիզոնական մասշտաբավորում՝ բազմակազմակերպական ծանրաբեռնվածության համար, առանց ծառայության ընդհատման թարմացումներ, ավտոմատ վերականգնում (Failover) և բեռնվածության բաշխում (Load Balancing):
Տեղակայման տարբերակներ (Packaging)	Լուծումը պետք է հնարավոր լինի տեղակայել ամպային (Cloud), տեղային (On-Premises) կամ մեկուսացված (Air-Gapped) միջավայրերում: Նախատիպը կարող է սկզբնական փուլում տրամադրվել SaaS կամ Cloud ձևաչափով, պայմանով, որ դիմորդը ներկայացնի հինգ տարվա իրատեսական ճանապարհային քարտեզ՝ անհրաժեշտության դեպքում ինքնիշխան, տեղային կամ մեկուսացված միջավայր տեղափոխելու համար:
Բազմավարձակալություն (Multi-Tenancy)	Յուրաքանչյուր կազմակերպության կամ պետական մարմնի տվյալների լիարժեք մեկուսացում, RBAC, MFA և նվազագույն անհրաժեշտ իրավունքների (Least Privilege) սկզբունքի կիրառում՝ տեղակայման բոլոր տարբերակներում:

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

Ոլորտ	Պահանջվող կարողություններ
Տվյալների ինքնիշխանություն (Data Sovereignty)	Տվյալները լռելյայն պետք է տեղակայվեն Հայաստանում (կամ ըստ սահմանված պահանջների):
Արտադրանքի անվտանգություն (Product Security)	Վերջից վերջ գաղտնագրում (պահպանման և փոխանցման ընթացքում), mTLS, սերտիֆիկատների կառավարում, API անվտանգության ապահովում, KMS, բանալիների պարբերական թարմացում, ինչպես նաև անվտանգ ծրագրային մշակման ստանդարտների (OWASP SAMM, NIST SSDF և այլն) կիրառում:
Համապատասխանություն (Compliance)	Համապատասխանություն SOC 2, ISO 27001 և SaaS լուծումների դեպքում՝ GDPR պահանջներին:
Աղետների վերականգնում (Disaster Recovery)	Փորձարկված պահուստավորման մեխանիզմներ՝ հստակ սահմանված RPO և RTO ցուցանիշներով:
DevOps հասունություն (DevOps Maturity)	CI/CD, դիտարկելիություն (Observability), միջադեպերի արձագանքման ընթացակարգեր (Runbooks) և KPI-ների շարունակական հաշվետվություն:
Ձեռնարկությունների աջակցություն (Enterprise Support)	Առնվազն 8×5 տեխնիկական աջակցություն՝ 24×7 սպասարկման անցնելու ճանապարհային քարտեզով և ISAA-ի կողմից հաստատված SLA-ներով:
Արտադրանքի կյանքի ցիկլ (Product Lifecycle)	Փաստաթղթավորված EOL (End of Life) և EOS (End of Support) քաղաքականություններ:

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

Ընդլայնված պահանջներ (պարտադիր)

Հատկանիշ	Նկարագրություն	Ակնկալվող արդյունք
Ամբողջականություն (Complete)	Բոլոր հայտնի սպառնալիքների և վերահսկողությունների ընդգրկում	IOC-ների և TTP-ների բացահայտում և վերլուծություն՝ պաշտպանության առավելագույն արդյունավետության ապահովման համար:
Կանխարգելիչ (Preemptive)	Անվտանգության բացերի հայտնաբերում մինչև դրանց շահագործումը	Կիբեռանվտանգության վերահսկողությունների թերությունների կանխարգելիչ հայտնաբերում և շտկում:
Շարունակականություն (Continuous)	Կիբեռպաշտպանության շարունակական ապահովում	Համակարգերի կարգավորումների մշտական թարմացում՝ նոր սպառնալիքներից պաշտպանվելու նպատակով:
Ստուգելիություն (Verifiable)	Ճշգրտության ձևական և դետերմինիստական ապացույցների ապահովում	Համակարգերում կատարված բոլոր փոփոխությունները պետք է լինեն անկախ ստուգման ենթակա՝ նվազեցնելով կեղծ դրական և կեղծ բացասական արդյունքները:

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

Հատկանիշ	Նկարագրություն	Ակնկալվող արդյունք
Համապարփակություն (Comprehensive)	Կիրառելիություն բազմաթիվ տեխնոլոգիական ոլորտներում և պաշտպանական սարքերում: Proof of Concept փուլում պարտադիր չէ աջակցել բոլոր արտադրատեսակներին, եթե ներկայացված է դրանց ընդլայնման իրատեսական ճանապարհային քարտեզ:	Աջակցություն առաջատար NGFW, IDS, IPS, EDR լուծումներին, ինչպես նաև նոր սարքատեսակների հետագա ինտեգրման ճանապարհային քարտեզ (օրինակ՝ Palo Alto, Fortinet, Cisco և այլն):

Առաջադեմ հատկանիշներին հասնելու համար կարող են կիրառվել հետևյալ մոտեցումները.

- կիբեռպաշտպանության միջոցների թվային երկվորյակների (Digital Twin) մոդելավորում՝ ներառյալ սպառնալիքների հայտնաբերման հնարավորությունները,
- կիբեռպաշտպանության միջոցների ձևական վավերացում (Formal Verification) կամ մոդելային ստուգում (Model Checking)՝ ներառյալ սպառնալիքների հայտնաբերման հնարավորությունները,
- կանխատեսող վերլուծություն և արհեստական բանականության վրա հիմնված կարգավորումների հավաստիության ապահովում,
- անվտանգության քաղաքականության կառավարման ինքնավար մեխանիզմներ,
- բարձր արագությամբ կարգավորումների համեմատություն և շեղումների (Configuration Drift) հայտնաբերում,
- բազմամատակարարային (Multi-vendor) աբստրակցիոն շերտեր,

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

- առաջադեմ սկանավորման, հեռաչափական (Telemetry) տվյալների համադրման կամ մոդելավորման միջավայրեր:

Դիմորդները պետք է իրենց նախատիպում ցուցադրեն առնվազն երեք առաջադեմ հատկանիշ՝ ներկայացնելով նաև դրանց ամբողջական համապատասխանության հասնելու իրատեսական ճանապարհային քարտեզ: Յուրաքանչյուր նախատիպ պետք է ներկայացնի կիբեռանվտանգության ապահովման ոլորտում հստակ և նշանակալի առաջընթաց:

Ցուցադրական կիրառման օրինակներ

1. Բազմամատակարարային համակարգերի կարգավորումների բազային վիճակի (Baseline) վերլուծություն:
2. Արտաքին հարձակման մակերեսի (External Attack Surface) կառավարման համապատասխանության ապահովում:
3. Անվտանգության քաղաքականությունների վերլուծություն՝ մարդկային սխալների կանխարգելման նպատակով:
4. Կանխարգելիչ կիբեռանվտանգության ապահովում:
5. Նորարարական լուծումներ (դիմորդի կողմից առաջարկվող մեթոդներ):

Մասնակի ֆունկցիոնալությամբ առաջարկների ներկայացումը թույլատրվում է:

Իրականացման ճանապարհային քարտեզի ֆունկցիոնալ պահանջներ

Դիմորդները պետք է ներկայացնեն KPI-ներ (արդյունավետության հիմնական ցուցանիշներ), որոնք կարտացոլեն առաջարկվող լուծման ամբողջականությունը, կանխարգելիչ բնույթը, շարունակականությունը, ստուգելիությունը և համապարփակությունը: Այն դեպքերում, երբ առաջարկվող այլ չափորոշիչներն ավելի արդյունավետ են արտացոլում ակնկալվող արդյունքները, դիմորդները կարող են ներկայացնել այլընտրանքային ցուցանիշներ:

Ցուցադրական օրինակներ.

1. Տարբեր տեսակի սարքերի կարգավորումների ընկալման և վերլուծության խորությունը:

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

2. Գլոբալ քաղաքականությունների հիման վրա իրականացվող չափումներ (օրինակ՝ բաց պորտերի համապատասխանություն, առավելագույն սկանավորվող IP հասցեների և պորտերի քանակ):
3. Մարդկային սխալները և դրանց շտկման ընթացքը ներկայացնող վահանակներ (Dashboards):
4. Հայտնի սպառնալիքների նկատմամբ կարգավորումների ծածկույթի և չծածկված սպառնալիքների պարբերական թարմացվող գնահատականներ:

Ակնկալվող արդյունքներ (Expected Deliverables)

Առաջարկների գնահատումը կիրականացվի մեկ գնահատման գործընթացի շրջանակում, որը ներառում է հետևյալ փուլերը.

Հայտի փաթեթ (Submission Package)

Դիմորդները պետք է ներկայացնեն՝

- տեխնիկական առաջարկ (առավելագույնը՝ 10 էջ),
- առկա նախատիպի նկարագրություն,
- լուծման ճարտարապետություն (Solution Architecture),
- հետազոտական և նորարարական մոտեցման նկարագրություն,
- հնգամյա առևտրայնացման (Commercialization) ճանապարհային քարտեզ,
- Առաջարկվող լուծման իրականացման բյուջե
- նախկինում իրականացված ցուցադրությունների վերաբերյալ ապացույցներ,
- փորձնական ներդրումների (Pilot Implementations) վերաբերյալ ապացույցներ (առկայության դեպքում),
- հաճախորդների երաշխավորագրեր (առկայության դեպքում),
- տեխնիկական տեսանյութեր (ըստ ցանկության),
- գիտական հրապարակումներ, արտոնագրեր կամ տեխնիկական հոդվածներ (առկայության դեպքում):

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

Նախնական ընտրություն (Shortlisting)

Գնահատող հանձնաժողովը կուսումնասիրի բոլոր ներկայացված հայտերը:

Գնահատող հանձնաժողովը իրավունք ունի 70 և ավել միավոր հավաքած մասնակիցներին հրավիրելու տեխնիկական ցուցադրության փուլ:

Տեխնիկական ցուցադրություն (Technical Demonstration)

Նախնական ընտրությունն անցած դիմորդները պետք է ներկայացնեն՝

- ուղիղ (Live) տեխնիկական ցուցադրություն,
- լուծման տեխնիկական ներկայացում (Technical Walkthrough),
- ճարտարապետական լուծման ներկայացում և քննարկում,
- պատասխաններ գնահատող հանձնաժողովի հարցերին,
- նորարարական բաղադրիչի ներկայացում,
- հետագա զարգացման ճանապարհային քարտեզ:

Վերջնական ընտրություն (Final Selection)

Տեխնիկական ցուցադրությունների ավարտից հետո Գնահատող հանձնաժողովը կընտրի մեկ դիմորդ կամ կարող է որոշում կայացնել որևէ դիմորդ չընտրելու վերաբերյալ:

Ֆինանսավորման ծավալ

- Սրցույթի շրջանակում տրամադրվող ֆինանսավորման ընդհանուր առավելագույն ծավալը կազմում է 100,000 (մեկ հարյուր հազար) ԱՄՆ դոլարին համարժեք ՀՀ դրամ՝ հաշվարկված ՀՀ կենտրոնական բանկի պայմանագրի կնքման օրվա պաշտոնական փոխարժեքով:
- Համաֆինանսավորմամբ և կոնսորցիումների կողմից ներկայացվող հայտերը խրախուսվում են, սակայն պարտադիր չեն:

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

Հնգամյա ճանապարհային քարտեզի (Roadmap) վերաբերյալ իրավասության պահանջներ

1. Ընդհանուր պահանջներ

- 3–4 ամսվա ընթացքում նախատիպ (Functional Prototype) մշակելու կարողություն,
- համապատասխան տեխնիկական կամ գիտահետազոտական փորձառություն,
- Հայաստանում անմիջականորեն կամ տեղական գործընկերոջ միջոցով գործունեություն իրականացնելու հնարավորություն,
- Հայաստանի կիբեռանվտանգության, տվյալների պաշտպանության և գաղտնիության վերաբերյալ օրենսդրության պահանջների պահպանում:

2. Ծրագրի տեսլական

- ազգային կիբեռպաշտպանության համակարգի նախագծման, մշակման և գործարկման հնգամյա փուլային նախաձեռնություն,
- ճանապարհային քարտեզ՝ ներառյալ Proof of Concept (PoC)-ի հիմնական փուլերը (milestones), հստակ նպատակները, չափելի հաջողության ցուցանիշները և ավարտի պայմանները,
- առաջատար լուծումների (օրինակ՝ NGFW, ZTNA, EDR, Cisco, Fortinet և այլն) ինտեգրում, ինչպես նաև այլ առաջադեմ հնարավորությունների ներդրում՝ ճկուն և դիմակայուն կիբեռանվտանգության ապահովման նպատակով:

ՄԱՍ 2

2. ՄԱՍՆԱԿՑԻ ՄԱՍՆԱԿՑՈՒԹՅԱՆ ԻՐԱՎՈՒՆՔԻ ՊԱՀԱՆՋՆԵՐԸ ԵՎ ԴՐԱՆՑ ԳՆԱՀԱՏՄԱՆ ՉԱՓՈՐՈՇԻՉՆԵՐԸ

2.1 Սույն ընթացակարգին մասնակցելու իրավունք չունեն անձինք.

1) որոնք հայտը ներկայացնելու օրվա դրությամբ դատական կարգով ճանաչվել են սնանկ.

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

2) որոնք կամ որոնց գործադիր մարմնի ներկայացուցիչը հայտը ներկայացնելու օրվան նախորդող հինգ տարիների ընթացքում դատապարտված է եղել ահաբեկչության ֆինանսավորման, երեխայի շահագործման կամ մարդկային թրաֆիքինգ ներառող հանցագործության, հանցավոր համագործակցություն ստեղծելու կամ դրան մասնակցելու, կաշառք ստանալու, կաշառք տալու կամ կաշառքի միջնորդության և օրենքով նախատեսված տնտեսական գործունեության դեմ ուղղված հանցագործությունների համար, բացառությամբ այն դեպքերի, երբ դատվածությունը օրենքով սահմանված կարգով մարված կամ վերացված է.

3) որոնց վերաբերյալ գնումների ոլորտում հակամրցակցային համաձայնության, գերիշխող դիրքի չարաշահման կամ անբարեխիղճ մրցակցության համար պատասխանատվություն սահմանող վարչական ակտը հայտը ներկայացվելու օրվան նախորդող երեք տարվա ընթացքում դարձել է անբողոքարկելի, իսկ բողոքարկված լինելու դեպքում թողնվել է անփոփոխ.

2.2. Արգելվում է սույն կետով սահմանված փոխկապակցված անձանց և (կամ) միևնույն անձի (անձանց) կողմից հիմնադրված կամ ավելի քան հիսուն տոկոս միևնույն անձի (անձանց) պատկանող բաժնեմաս (փայաբաժին) ունեցող կազմակերպությունների միաժամանակյա մասնակցությունը սույն ընթացակարգին (միևնույն չափաբաժնին)

Սույն կետի իմաստով՝

1) Ֆիզիկական անձինք համարվում են փոխկապակցված, եթե նրանք միևնույն ընտանիքի անդամ են կամ վարում են ընդհանուր տնտեսություն կամ համատեղ ձեռնարկատիրական գործունեություն կամ գործել են համաձայնեցված՝ ելնելով ընդհանուր տնտեսական շահերից

2) Ֆիզիկական և իրավաբանական անձինք համարվում են փոխկապակցված, եթե նրանք գործել են համաձայնեցված՝ ելնելով ընդհանուր տնտեսական շահերից, կամ եթե տվյալ ֆիզիկական անձը կամ նրա ընտանիքի անդամը հանդիսանում է՝

ա. տվյալ իրավաբանական անձի բաժնետոմսերի տաս տոկոսից ավելին տնօրինող մասնակից.

բ. ՀՀ օրենսդրությամբ չարգելված այլ ձևով իրավաբանական անձի որոշումները կանխորոշելու հնարավորություն ունեցող անձ.

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

գ. տվյալ իրավաբանական անձի խորհրդի նախագահ, խորհրդի նախագահի տեղակալ, խորհրդի անդամ, գործադիր տնօրեն, նրա տեղակալ, գործադիր մարմնի գործառույթներ իրականացնող կոլեգիալ մարմնի նախագահ, անդամ,

դ. իրավաբանական մարմնի այնպիսի աշխատակից, որն աշխատում է գործադիր տնօրենի անմիջական ղեկավարության ներքո կամ իրավաբանական անձի կառավարման մարմինների կողմից որոշումների կայացման հարցում որևէ էական ազդեցություն ունի:

3) Ֆիզիկական անձի կարգավիճակ չունեցող մասնակիցները համարվում են փոխկապակցված, եթե

ա. տվյալ իրավաբանական անձը քվեարկելու իրավունքով տիրապետում է մյուսի՝ ձայնի իրավունք տվող բաժնետոմսերի (բաժնեմասերի, փայերի) տասը և ավելի տոկոսին, կամ իր մասնակցության ուժով կամ տվյալ անձանց միջև կնքված պայմանագրին համապատասխան՝ հնարավորություն ունի կանխորոշելու մյուսի որոշումները.

բ. նրանցից մեկի ձայնի իրավունք տվող բաժնետոմսերի քսան տոկոսից ավելիին տիրապետող կամ օրենքով չարգելված այլ ձևով նրա որոշումները կանխորոշելու հնարավորություն ունեցող մասնակից(ներ)ը (բաժնետեր(եր)ը) կամ նրանց ընտանիքի անդամներն իրավունք ունեն ուղղակի կամ անուղղակի կերպով տիրապետելու (այդ թվում՝ առուվաճառքի, հավատարմագրային կառավարման, համատեղ գործունեության, հանձնարարության պայմանագրերի կամ այլ գործարքների հիման վրա) մյուս անձի՝ ձայնի իրավունք տվող բաժնետոմսերի քսան տոկոսից ավելիին կամ ունեն օրենքով չարգելված այլ ձևով վերջինիս որոշումները կանխորոշելու հնարավորություն.

գ. նրանցից մեկի որևէ կառավարման մարմնի կամ նման պարտականություններ կատարող այլ անձանց, ինչպես նաև նրանց ընտանիքի անդամների թվի մեկ երրորդը միաժամանակ հանդիսանում է մյուս անձի որևէ կառավարման մարմնի անդամ կամ նման պարտականություններ կատարող այլ անձ.

դ. նրանք գործել են համաձայնեցված՝ ելնելով ընդհանուր տնտեսական շահերից:

Սույն կետի իմաստով ընտանիքի անդամ են համարվում հայրը, մայրը, ամուսինը ամուսնու ծնողները, տատը, պապը, քույրը, եղբայրը, երեխաները, քրոջ կամ եղբոր ամուսինն ու երեխաները:

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

2.3 **Սույն ընթացակարգին մասնակցող ընկերությունների և մատուցվելիք ծառայությունների նկատմամբ նվազագույն պահանջներ.**

Սույն տեխնիկական առաջադրանքով նախատեսված դրամաշնորհի մրցույթին հայտ կարող են ներկայացնել այն իրավաբանական անձինք, որոնք մասնավոր հատվածի կազմակերպություններ են (ստարտափներ, փոքր և միջին ձեռնարկություններ, ինչպես նաև կայացած լուծումներ տրամադրող ընկերություններ),

- հետազոտական և իրականացման կարողությունները համատեղող կոնսորցիումները,
- համալսարանները, գիտահետազոտական լաբորատորիաները և ակադեմիական կենտրոնները,
- քաղաքացիական հասարակության կազմակերպությունները և վերլուծական (think tank) կենտրոնները:

Նախապատվություն կտրվի՝

- Հայաստանում գրանցված կամ հայկական ֆինանսավորմամբ ընկերություններին (սակայն մասնակցությունը չի սահմանափակվում մյուս կազմակերպությունների համար),
- Հայաստանում գործունեության նախկին փորձ ունեցող կազմակերպություններին,
- տեղական և միջազգային գործընկերների մասնակցությամբ ձևավորված կոնսորցիումներին, որոնք ունեն փոխլրացնող փորձ և մասնագիտական կարողություններ:

2.4 Սույն ընթացակարգին մասնակցող կազմակերպությունների կողմից 2.3 կետում նշված պայմաններին բավարարելու դեպքում, մասնակցող ընկերությունները գնահատվում են ըստ առավելություն տվող չափորոշիչների՝ համաձայն 2.5 կետում նշված կշիռների:

2.5. Գնահատման չափանիշներն ու մեթոդաբանությունը

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

Առաջարկների գնահատումն իրականացվում է Գնահատող հանձնաժողովի կողմից՝ կշռված գնահատման մեթոդով՝ համաձայն ստորև ներկայացված չափանիշների և դրանց կշիռների:

Յուրաքանչյուր չափանիշ գնահատվում է 0-ից 5 միավոր սանդղակով՝ հետևյալ գնահատականների համաձայն.

Միավոր	Գնահատման նկարագրություն
0	Չի ներկայացվել կամ ամբողջությամբ չի համապատասխանում տվյալ չափանիշի պահանջներին:
1	Ներկայացված է շատ թույլ, բավարար հիմնավորումներ կամ ապացույցներ չեն ներկայացվել:
2	Մասնակիորեն համապատասխանում է պահանջներին, սակայն առկա են էական բացեր, որոնք կարող են ազդել ծրագրի հաջող իրականացման վրա:
3	Համապատասխանում է սահմանված նվազագույն պահանջներին, ներկայացված են բավարար հիմնավորումներ և ապացույցներ:
4	Գերազանցում է նվազագույն պահանջները, ներկայացված են համոզիչ տեխնիկական հիմնավորումներ, հստակ առավելություններ և իրագործելի իրականացման մոտեցում:
5	Բացառիկ որակի առաջարկ է, որը ցուցադրում է բարձր նորարարություն, տեխնիկական հասունություն, պետական հատվածում կիրառման հստակ ներուժ և ներկայացված է բավարար ու վստահելի ապացույցներով:

Գնահատման չափանիշները

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

Չափանիշ	Կշիռ
Հայաստանի կիբեռանվտանգության ռազմավարական առաջնահերթություններին համապատասխանություն	20%
Նորարարական մոտեցում և տեխնիկական տարբերակվածություն	20%
Առկա նախատիպի տեխնիկական հասունություն	20%
Կենդանի (Live) տեխնիկական ցուցադրություն	20%
Նախկինում իրականացված Proof of Concept-ներ (PoC), պիլոտային ծրագրեր կամ վաղ կիրառման փորձ	10%
Թիմի մասնագիտական կարողություններ և իրականացման ներուժ	10%

Գնահատման կարգ

- Գնահատող հանձնաժողովի յուրաքանչյուր անդամ յուրաքանչյուր չափանիշի համար շնորհում է 0–5 միավոր:
- Յուրաքանչյուր չափանիշի վերջնական միավորը հաշվարկվում է հանձնաժողովի անդամների կողմից տրված միավորների միջին թվաբանականի հիման վրա:
- Վերջնական գնահատականը հաշվարկվում է յուրաքանչյուր չափանիշի միջին միավորը համապատասխան կշռով բազմապատկելու միջոցով:

Վերջնական գնահատականը հաշվարկվում է հետևյալ բանաձևով.

Կշռված միավոր = (Չափանիշի համար ստացված միավոր ÷ 5) × Չափանիշի կշիռ

Լրացուցիչ դրույթներ

Գնահատման ընթացքում հանձնաժողովն իրավունք ունի.

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

- պահանջելու լրացուցիչ պարզաբանումներ կամ հիմնավորող փաստաթղթեր,
- կազմակերպելու լրացուցիչ տեխնիկական ցուցադրություն,
- ստուգելու ներկայացված տեղեկությունների արժանահավատությունը,
- դիմելու անկախ տեխնիկական կամ ոլորտային փորձագետների խորհրդատվությանը:
- անհրաժեշտության դեպքում հիմնավորված կերպով փոփոխել գնահատման ժամանակացույցը,
- բանակցել ծրագրի շրջանակի, փուլային արդյունքների (milestones), բյուջեի, առևտրային պայմանների և իրականացման մոտեցման վերաբերյալ,

---

Ֆինանսավորման համար կարող են դիտարկվել միայն այն առաջարկները, որոնք ստացել են առնվազն 70 միավոր (100-ից):

Առաջարկի վերջնական գնահատականը հավասար է բոլոր չափանիշների կշռված միավորների գումարին: Առավելագույն հնարավոր գնահատականը 100 միավոր է:

Առավելագույն միավոր հավաքած առաջարկը ճանաչվում է հաղթող:

Ընդհանուր կամ տեսական բնույթի առաջարկները կարող են ստանալ ավելի ցածր գնահատական, նույնիսկ եթե տեխնիկական առումով հիմնավորված են:

ՄԱՍ 3
3. ՀՐԱՎԵՐՈՒՄ ԵՎ ՀԱՅՏԵՐՈՒՄ ՓՈՓՈԽՈՒԹՅՈՒՆ ԿԱՏԱՐԵԼՈՒ ԿԱՐԳԸ

3.1 Հրավերում փոփոխությունները կարող են կատարվել մինչև հայտերի բացման օրը: Հրավերում փոփոխություններ կատարելու դեպքում մասնակիցներն իրավունք ունեն սույն կանոնակարգով սահմանված կարգով հայտերում կատարել լրացուցիչ

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

փոփոխություններ: Հիմնադրամը հրավերում փոփոխության կատարման դեպքում չի կրում փոփոխության արդյունքում մասնակիցների կրած իրական վնասների ռիսկը:

3.2 Մասնակիցները մինչև հայտերը ներկայացնելու վերջնական ժամկետի ավարտը կարող են փոխել կամ հետ վերցնել հայտերը: Առաջարկների փոփոխումը կատարվում է սույն կանոնակարգով սահմանված Առաջարկների ներկայացնելու համար նախատեսված կարգով: Մասնակիցները նույն կարգով կարող են հետ վերցնել Առաջարկներըրը, մասնավորապես հրավերի 4.2-րդ կետում նշված հասցեին ներկայացնելով դիմում Առաջարկները հետ վերցնելու կամ փոփոխելու վերաբերյալ:

ՄԱՍ 4
4. ՀԱՅՏԸ ՆԵՐԿԱՅԱՑՆԵԼՈՒ ԿԱՐԳԸ

4.1 Առաջարկները մասնակիցները ներկայացնում են՝

- Էլեկտրոնային փոստի միջոցով՝

4.2 Առաջարկները և սույն հրավերով սահմանված փաստաթղթերը էլեկտրոնային եղանակով ներկայացվում են procurement@isaa.am էլ. փոստին մինչև 2026 թվականի սեպտեմբերի 2-ը՝ ժամը 11:00: Փաստաթղթերն անհրաժեշտ է ուղարկել pdf ֆորմատով, խմբավորված, վերնագիր դաշտում նշելով՝ «Կիբեռանվտանգության նորարարական ցուցադրական դրամաշնորհի մրցույթ»:

4.3 Գնահատման փուլում գնահատող հանձնաժողովի կողմից կարող են պահանջվել ներկայացված փաստաթղթերի բնօրինակները:

4.4 Մասնակիցը չի կարող նույն մրցույթի շրջանակներում ներկայացնել մեկից ավելի Առաջարկ: Նույն մրցույթի շրջանակներում Մասնակցի կողմից ներկայացված բոլոր հայտերը հանդիսանում են անվավեր և չեն դիտարկվում:

4.5 Հայտը և կից փաստաթղթերը՝

Հավելված 2
Հայտի օրինակելի ձև

Պահանջվող տեղեկատվություն	**Մանրամասներ**
Մասնակից Կազմակերպության անվանումը	

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

Պետական գրանցման համարը	
Գործունեության հասցե	
Բջջային հեռախոսահամար	
ՀՎՀՀ	
Հայտը ստորագրող անձի անուն ազգանուն	
Հայտը ստորագրող անձի անձնագրի կամ նույնականացման քարտի տվյալները	
Հայտը ստորագրող անձի պաշտոնը մասնակից կազմակերպությունում՝	
Հայտի լրացման ամսաթիվ	
Հայտը լրացնող անձի ստորագրությունը	
Առաջարկվող լուծման իրականացման բյուջե (ՀՀ դրամով)	

Սույն տեխնիկական առաջադրանքի 2.3-րդ, 2.5-րդ կետերով սահմանված պահանջների և գնահատման չափանիշների համապատասխանությունը հավաստիացնելու նպատակով, մասնակից կազմակերպությունը պարտավոր է հայտին կից ներկայացնել հետևյալ հիմնավորող փաստաթղթերը.

- տեխնիկական առաջարկ (առավելագույնը՝ 10 էջ),
- առկա նախատիպի նկարագրություն,
- լուծման ճարտարապետություն (Solution Architecture),
- հետազոտական և նորարարական մոտեցման նկարագրություն,
- հնգամյա առևտրայնացման (Commercialization) ճանապարհային քարտեզ,
- նախկինում իրականացված ցուցադրությունների վերաբերյալ ապացույցներ,
- փորձնական ներդրումների (Pilot Implementations) վերաբերյալ ապացույցներ (առկայության դեպքում),
- հաճախորդների երաշխավորագրեր (առկայության դեպքում),
- տեխնիկական տեսանյութեր (ըստ ցանկության),

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

- գիտական հրապարակումներ, արտոնագրեր կամ տեխնիկական հոդվածներ (առկայության դեպքում):
- PoC-ների, պիլոտային ծրագրերի կամ վաղ կիրառման փորձը հավաստող փաստաթղթեր,
- Թիմի կազմը, հիմնական մասնագետների CV-ները և համապատասխան փորձը ներկայացնող տեղեկատվություն:

Արհեստական բանականություն (AI) ներառող լուծումները պետք է լինեն բավարար չափով թափանցիկ, որպեսզի Գնահատման հանձնաժողովը կարողանա իրականացնել դրանց անկախ տեխնիկական գնահատումը:

Հանձնաժողովի պահանջով հայտատուները պարտավոր են տրամադրել մուտք լուծման հիմքում ընկած իրականացմանը՝ ներառյալ սկզբնաղբյուր կոդի (source code) ներկայացում և ուսումնասիրություն (walkthrough), մոդելի փաստաթղթավորում, կիրառված ալգորիթմներ, ուսուցման և վավերացման (training and validation) մեթոդաբանություններ, տվյալների հավաքածուներ (այն դեպքերում, երբ դա թույլատրվում է օրենսդրությամբ), մոդելի գնահատման արդյունքներ, ինչպես նաև այլ տեխնիկական նյութեր, որոնք անհրաժեշտ են առաջարկվող լուծման գիտական հիմնավորվածությունը, ճշտությունը, կայունությունը (robustness) և արդյունավետությունը գնահատելու և հաստատելու համար: Միայն «սև արկղի» (black-box) սկզբունքով իրականացվող ցուցադրությունները, որոնք չեն ապահովում բավարար տեխնիկական թափանցիկություն, կարող են համարվել գնահատման համար անբավարար:

Սույն հրավերով պահանջվող հիմնավորող փաստաթղթերի չներկայացումը կամ ոչ բավարար լինելը հանդիսանում է հայտի մերժման հիմք: Հայտը և կից փաստաթղթերը կարող են ներկայացվել հայերեն կամ անգլերեն լեզուներով:

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

ՄԱՍ 5

5. Հայտերի բացումը, գնահատումը և արդյունքների ամփոփումը

5.1 Առաջարկները ներկայացնելու վերջնաժամկետն է 2026թ. սեպտեմբերի 2-ը՝ ժամը 11:00: Առաջարկների բացման համար սահմանված օրը և ժամին՝ Վազգեն Սագսյան 26/1, 400 գրասենյակ հասցեում, 2026թ սեպտեմբերի 2-ին ժամը 11:00-ին: Սույն հրավերի վերաբերյալ պարզաբանումներ ստանալու նպատակով հարցեր կարող են ներկայացվել մինչև 2026 թվականի օգոստոսի 25-ը՝ ժամը 18:00-ն՝ procurement@isaa.am էլեկտրոնային փոստի հասցեին:

Հիմնադրամի գնումների մասնագետը կկազմի ներկայացված հայտերի վերաբերյալ ամփոփ տեղեկանք:

5.2 Հայտերով ներկայացված առաջարկները 5.1 կետով սահմանված տեղեկանքի հիման վրա քննարկվում և ամփոփվում են Հանձնաժողովի հայտերի քննարկման և ամփոփման նիստում՝ մինչև 2026թ սեպտեմբերի 10-ը:

5.3 Մրցութային հանձնաժողովը քննարկման և ամփոփման նիստի ավարտից հետո 2 (երկու) աշխատանքային օրվա ընթացքում կկազմվի առաջարկների արդյունների մասին արձանագրություն, որտեղ նշված կլինի հետևյալը՝

- առաջարկների բացման, ինչպես նաև դրանց ամփոփման վայրը, ամսաթիվը և ժամը, ինչպես նաև մրցութային հանձնաժողովի անդամների, նիստին մասնակցող հրավիրված մասնագետների անունները, ազգանունները, պաշտոնները
- առաջարկների վերաբերյալ տեղեկություններ
- Մրցույթում հաղթողի անունը/անվանումը
- Այն չափորոշիչները, որոնց հիման վրա մրցույթի մասնակիցներից մեկը հաղթող է ճանաչվել
- Այլ անհրաժեշտ տեղեկատվություն

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am

ՄԱՍ 6

6. ՊԱՅՄԱՆԱԳՐԻ ԿՆՔՈՒՄ

6.1 Մրցույթում հաղթող ճանաչված մասնակիցի հետ մրցույթի ամփոփումից հետո 5 աշխատանքային օրվա ընթացքում կնքվում է պայմանագիր:

6.2 Մրցույթում հաղթող ճանաչված մասնակիցի հետ 6.1 կետում սահմանված ժամկետում պայմանագիր չկնքելու դեպքում, Հիմնադրամը գնման պայմանագրի առաջարկ է ներկայացնում մրցույթում երկրորդ, իսկ վերջինիս կողմից առաջարկը չընդունվելու դեպքում՝ երրորդ տեղը զբաղեցրած մասնակցին:

ՄԱՍ 7

ԸՆԹԱՑԱԿԱՐԳԸ ՉԿԱՅԱՑԱԾ ՀԱՅՏԱՐԱՐԵԼԸ

7.1 Մրցույթը համարվում է չկայացած, եթե՝

1. մրցույթին չի ներկայացվել ոչ մի առաջարկ,
2. ներկայացված բոլոր առաջարկները չեն համապատասխանում սույն հայտարարությամբ սահմանված պահանջներին,
3. մրցութային հանձնաժողովի կողմից չի որոշվել հաղթող՝ առաջարկների անհամապատասխանության կամ գնահատման արդյունքների հիման վրա,
4. մրցույթի հաղթողը հրաժարվել է պայմանագրի կնքումից, և սույն հրավերի 6.2 կետով սահմանված կարգով նոր հաղթող չի հայտարարվել,
5. մասնակիցները չեն պահպանել սույն հայտարարությամբ սահմանված այլ պարտադիր պահանջները:

7.2 Սույն կետով նախատեսված դեպքերում Պատվիրատուն իրավունք ունի մրցույթը հայտարարել չկայացած՝ առանց որևէ պարտավորության կամ փոխհատուցման մասնակիցների նկատմամբ:

7.3 Կեղծ, խեղաթյուրված կամ մոլորեցնող տեղեկատվության ներկայացման դեպքում Հիմնադրամը իրավունք ունի մերժել մասնակցի հայտը ցանկացած փուլում:

Վազգեն Սարգսյան 26/1, 0010 Երևան info@isaa.am