

Приложение № 2

към рамков договор № № 93-00-97 от 03.07.2020 г.

ЗАЯВКА по Рамков договор № 93-00-97 от 03.07.2020 г. (вх. № ПО-16-875/03.07.2020 г. на ИО АД)		<input type="checkbox"/>
ЗАЯВКА по Рамков договор № 93-00-97 от 03.07.2020 г. (вх. № ПО-16-875/03.07.2020 г. на ИО АД) (актуализирана)		<input checked="" type="checkbox"/> ¹
Позиция от ПГ-2024 г.:	№ по ред от ПГ	16
Описание на проект съгласно ПГ:	Доставка на ИКТ решение с цел надграждане на инфраструктура ориентирана към приложенията между ИЦ и РИЦ	
CPV код	32420000-3	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	МЕУ-19807/19.12.2025	
Изискване за достъп до класифицирана информация ДА/НЕ	НЕ	
Стойност: (стойността следва да съответства на заложената в План-графика) без ДДС, в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово	1 063 630,00 лв. без ДДС	
Начин за плащане: (еднократно, на части, периодично, авансово или др.)	Еднократно, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършената доставка/дейност и фактура.	
Плащане с акредитив или авансово ДА/НЕ	ДА	
Документи за плащане с акредитив или авансово	Съгласно изискването на акредитива	
Срок на изпълнение: (от дата – до дата или в месеци, ако не е обвързан с конкретна дата)	Срок за доставка – до 120 дни след получаване на уведомление за осигурено финансиране от страна на Възложителя.	
Гаранционен срок: (от дата – до дата или в месеци, ако не е обвързан с конкретна дата)	Съгласно условията на ТС	
Отчитане: (периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)	Еднократно, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършената доставка/дейност.	
Приложения: (напр: технически параметри, образци на отчетни документи)	Технически параметри	
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА ОТ:		
Ръководител на проект по заявката от страна на БЕНЕФИЦИЕРА (напр: представител на дирекцията – Заявител):		
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:		Подпис:

¹ Отбелязва се в случай че заявката е актуализирана

Ръководител на договора от страна на БЕНЕФИЦИЕРА:		<i>Подпис:</i>
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Ръководител на проект по заявката		<i>Подпис:</i>
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		<i>Подпис:</i> ▲ ◀ ▶

Забележка: С една заявка могат да се възлагат повече от един проект по ППГ, само когато те са еднотипни и управлението им (възлагане, изпълнение, отчитане) може да се извършва съгласно описанията в таблицата от заглавната страница на заявката параметри и лица. В този случай в таблицата се добавят необходимия брой редове, за описване на съответните проекти. Когато проектите не са еднотипни, те се възлагат с отделни заявки.

Заличаванията в документите са на основание чл. 4 от Общия регламент относно защитата на данните - Регламент (ЕС) 2016/679

ТЕХНИЧЕСКИ ПАРАМЕТРИ

За доставка на ИКТ решение с цел изграждане на инфраструктура ориентирана към приложенията между ИЦ и РИЦ

1. Обект на заявката

Обекта на заявката съгласно Общия терминологичен речник – CPV е с код, както следва:

CPV код	Описание
32420000-3	Мрежово оборудване

2. Обща информация

Агенция по вписванията поддържа и развива информационни системи от национално значение. За поддържане на високите нива за отказоустойчивост е необходимо да се закупи хардуерно и софтуерно решение, с което да се награди текущата инфраструктура като се изгради единна хомогенна инфраструктура. Това решение е необходимо за да може да се осигури безпроблемното преместване на сървъри между различните центрове за данни без да се нарушава работоспособността на системите, администрирани от Агенция по вписванията

3. Предмет

Настоящата заявка обхваща:

- Доставка на хардуерно и софтуерно оборудване, както следва:

Минимални технически изисквания	
Шаси/кутия и захранване:	
REQ. 1	Всички физически устройства трябва да позволяват директен монтаж в 19“ шкаф. За целите на монтажа да бъдат осигурени всички необходими крепежни елементи, захранващи и мрежови кабели.
REQ. 2	Всички физически осем устройства трябва да имат минимум два токозахранващи модула, работещи в режим с пълно резервиране. Да поддържат захранване от 220-240v AC, 50Hz.
REQ. 3	Всяко от физически устройства трябва да имат минимум един 10/100/1000BASE-T и един сериен интерфейс (конзола) за управление (ООВ).
REQ. 4	Всички физически устройства трябва да имат минимум един USB порт.
Основни функции:	

REQ. 5	<p>Предложеното решение за SDN (Software Defined Network) трябва да включва минимално следните компоненти:</p> <ul style="list-style-type: none"> - Резервиран клъстер от минимум три виртуални контролера разположени върху физически сървъри осигурени от Възложителя в основен и резервен център за данни. - Виртуалните контролери да са съвместими с VMware ESXi инфраструктура - Фабрика от два опорни (Spine) комутатора и два крайни (Leaf) комутатора за основен център за данни. - Фабрика от два опорни (Spine) комутатора и два крайни (Leaf) комутатора за резервен център за данни. - Опорните комутатори трябва имат минимум 32 x 400 Gbps QSFP-DD и 2 x 1/10 Gbps SFP+ интерфейса . - Крайните комутатори трябва да имат минимум 8 x 100/400 Gbps QSFP-DD и 28 x 40/100 Gbps QSFP28 интерфейса.
REQ. 6	<p>Решението трябва да преизползва съществуващите четири Cisco Nexus 93180YC-FX комутатори за връзка между основен и резервен център за данни. За целта е необходимо да се осигурят следните лицензи и трансивери.</p> <p>C1A1TN9300XF DCN Advantage License – 4 броя</p> <p>C1-N9K-SEC-XF Data Center Networking Security License (MACSEC) – 4 броя</p> <p>QSFP-100G-ERL-S 100G QSFP28 Transceiver 100G ER-Lite, 25km SMF, duplex, LC – 4 броя</p> <p>QSFP-100G-B20U4-I 100GBASE QSFP Transceiver BD 20km upstream LC Simplex SMF – 1 брой</p> <p>QSFP-100G-B20D4-I 100GBASE QSFP Transceiver, BD 20km downstream LC Simplex SMF – 1 брой</p>
REQ. 7	<p>Към комутаторите трябва да се осигурят минимум следните трансивери (общо за цялото решение):</p> <p>100G DAC QSFP кабел с дължина 10 метра – 16 броя.</p> <p>100G DAC QSFP кабел с дължина 5 метра – 8 броя.</p> <p>400G DAC QSFP кабел с дължина 3 метра – 8 броя.</p> <p>400G DAC QSFP кабел с дължина 2.5 метра – 8 броя.</p> <p>10G DAC SFP+ кабел с дължина 3 метра – 8 броя.</p> <p>10G DAC SFP+ кабел с дължина 5 метра – 8 броя.</p> <p>100G QSFP to 4 x 25G SFP кабел с дължина 3 метра – 4 броя.</p> <p>QSFP to 4 x 10G SFP кабел с дължина 3 метра – 2 броя.</p> <p>QSFP to 4 x 10G SFP кабел с дължина 5 метра – 2 броя.</p> <p>Всички трансивери трябва да са съвместими с предложеното оборудване.</p>
REQ. 8	<p>Всички комутатори трябва да имат неблокируема архитектура.</p>
REQ. 9	<p>Комутаторите трябва да поддържат Spine/Leaf топология на две нива.</p>
REQ. 10	<p>Предложеното решение трябва да е напълно резервирано. Работа на системата трябва да продължи при отпадане на който и да е единичен компонент.</p>

REQ. 11	Предложеното решение изисква пълна резервираност за връзката между основен и резервен център за данни. Необходимо е да се поддържат две криптирани 100Gbps връзки посредством осигурените трансивери от REQ. 7. Комутаторите за осигуряване на връзка между основен и резервен център за данни трябва да поддържат криптиране IEEE 802.1ae (MACSEC) без загуба на производителност.
REQ. 12	Отпадането или добавяне на контролер не трябва да нарушава работата на системата. Отпадането дори на всички контролери не трябва да спира работата на вече провизираните услуги.
REQ. 13	Решението трябва да поддържа IPv4 и IPv6.
REQ. 14	Опорните комутатори и крайните комутатори трябва да имат възможност за добавяне директно или чрез допълнителен лиценз на IEEE 802.1ae (MACSEC).
REQ. 15	Предложеното решение трябва да позволява увеличаване на производителността чрез добавяне на Spine комутатори (до шест броя общо).
REQ. 16	Предложеното решение трябва да позволява увеличаване на капацитета чрез добавяне на Leaf комутатори (до двадесет и четири броя от предложеният тип общо).
REQ. 17	Предложеното решение трябва да позволява добавяне или премахване на компоненти от фабриката (контролери, комутатори) без прекъсване на услугите.
REQ. 18	Предложеното решение трябва да поддържа технология за виртуализация на мрежата - VxLAN.
REQ. 19	Предложеното решение трябва да поддържа технология за разтегляне на Layer 2 VLAN мрежи между два и повече центъра за данни, позволявайки миграция на сървъри и виртуални машини без промяна на адресната им схема.
REQ. 20	Мрежовата архитектура трябва да поддържа "VxLAN overlay" в хардуера за да осигурява логически топологии и абстракция на хардуера без загуба на производителност.
REQ. 21	Решението трябва да поддържа "multi-home" и "multi-pathing" при бъдещо разширение към допълнителни центрове за данни за ефективно използване на капацитета на всички активни връзки.
REQ. 22	Решението трябва да поддържа отдалечени крайни комутатори през IP свързаност.
REQ. 23	Решението трябва да позволява разширение до три центъра за данни с добавяне единствено на комутатори и без допълнителна инвестиция за контролери.
REQ. 24	Решението трябва да позволява връзка към други фабрики/кълъстери с възможност за централизирано управление.
REQ. 25	Решението трябва да притежава средства за контрол на BUM (broadcast, unknown unicast, multicast) трафика.
REQ. 26	Решението трябва да позволява интеграция с L4-7 устройства (защитни стени, IPS/IDS-и, loadbalancer-и и др.).
REQ. 27	Решението трябва да позволява интеграция със защитни стени в „transparent” или „routed” режим, изпълнени както с хардуерни така и виртуални защитни стени.
REQ. 28	Решението трябва да позволява интеграция с хипервайзори на VMware, Microsoft и Redhat.

REQ. 29	Трафика от виртуални машини и физически сървъри трябва да подлежи на идентичен контрол.
REQ. 30	Решението трябва да поддържа провизиране и наблюдение на порт групи на виртуални машини на различни хипервизори.
REQ. 31	Решението трябва да поддържа преместване на виртуални машини на различни производители (Vmware, Microsoft, Redhat) между произволни точки от фабриката.
REQ. 32	Решението трябва да наблюдава и визуализира чрез контролера загуби на пакети и закъснения.
REQ. 33	Фабриката трябва да балансира автоматично трафика с пренасочване към по-слабо натоварени връзки при пикови натоварвания.
REQ. 34	Фабриката трябва да приоритизира по-леките потоци от информация за сметка на по-тежките.
REQ. 35	Решението трябва да поддържа дистрибутиран шлюз по подразбиране (default gateway) на всеки краен комутатор. Ако е необходима маршрутизация тя трябва да се извършва още на първият комутатор от фабриката през който влиза трафика.
REQ. 36	Решението трябва да поддържа множество връзки към външни мрежи с поддръжка на BGP, OSPF и статична маршрутизация. Трябва да се поддържат филтри (префикс листи) входящо и изходящо от фабриката.
REQ. 37	Научаването на MAC, IP, VTEP ID, трябва да става в хардуера на фабриката с цел по-добра производителност.
REQ. 38	Решението трябва да поддържа DHCP relay.
REQ. 39	Решението трябва да поддържа изолация на сървъри в един мрежов сегмент независимо дали са физически или виртуални.
REQ. 40	Решението трябва да поддържа списъци за контрол на достъпа (ACL) между сървъри или група независимо дали са физически или виртуални.
REQ. 41	Решението трябва да поддържа хостове закачени към два различни комутатора за резервиране чрез MCEC (Multi-chassis etherchannel) технология. Трябва да се поддържа LACP протокол.
Управление и наблюдение:	
REQ. 42	Цялата фабрика трябва да се менажира като един логически компонент.
REQ. 43	Клъстера от контролери трябва да се синхронизира автоматично. Трябва да притежава решение при евентуален „split-brain” сценарий.
REQ. 44	Решението трябва да позволява логическо разделение на системата между различни ползватели (multi-tenancy) със напълно самостоятелна политика. Трафик между различни ползватели (tenants) трябва да е възможен само по контролиран път през защитни стени.

REQ. 45	Решението трябва да позволява автоматизирано (zero-touch) провизиране на комутатори.
REQ. 46	Решението трябва да поддържа автоматично откриване на топологията на фабриката по LLDP и визуализирането и през контролерите.
REQ. 47	Решението трябва да е програмируемо с възможност за промени през отворен програмен интерфейс (API). Достъпа до API трябва да е ограничен единствено през една точка (кълстера от контролери). Трябва да могат да се поддържат оркестратори и системи за управление на други производители.
REQ. 48	Решението трябва да поддържа функции за анализ на трафика, трафични статистики, улавяне на пакети.
REQ. 49	Решението трябва да позволява доклади за състоянието на системата.
REQ. 50	Решението трябва да поддържа SNMP протокол.
REQ. 51	Решението трябва да поддържа TACACS+, RADIUS, LDAP и локална автентикация. Решението трябва да може да се интегрира с активна директория посредством LDAP протокол.
REQ. 52	Решението трябва да поддържа роли ограничаващи достъпа на потребителите на системата само до определени функции.
REQ. 53	Решението трябва да поддържа двуфакторна автентикация.
REQ. 54	Решението трябва да открива аномалии на база телеметрични данни с което да помага за бързото откриване и решаване на проблеми с „control-plane“ трафика.
REQ. 55	Решението трябва да може да мониторира ресурсите на фабриката, да показва тенденции, както и да открива компоненти с високо натоварване.
REQ. 56	Решението трябва да може да открива аномалии в хардуерни компоненти като CPU, памет, температура, обороти на вентилаторите.
REQ. 57	Решението трябва да поддържа автоматично провизиране на услуги през RESTful API в JSON и XML формат.
REQ. 58	Фабриката трябва да поддържа различни опции за програмируемост: python, bash, netconf, xml/json.
REQ. 59	Доставчикът трябва да осигури безплатно симулатор на софтуера на контролера (виртуална машина или хардуер) който може да се използва за тестове и обучение.
REQ. 60	Контролерът трябва да поддържа CLI интерфейс за цялостно конфигуриране на фабриката. Конфигурацията трябва да се синхронизира с GUI интерфейса.
REQ. 61	Комутаторите трябва да поддържат CLI интерфейс за мониторинг и откриване на проблеми.
REQ. 62	Контролерът трябва да запазва конфигурацията на регулярни интервали или при команда и да може да възстановява стара такава при необходимост.

REQ. 63	Да се предвиди софтуер за мониториране на системата след първоначална инсталация (Day 2 Ops) за проактивно откриване и отстраняване на проблеми в системата. Софтуера се допуска да работи върху контролерите или върху отделна виртуална машина.
Гаранция и поддръжка:	
REQ. 64	Срок на техническа поддръжка директно от производителя – минимум 3 (три) години.
REQ. 65	Получаване на нови версии на софтуера - минимум 3 (три) години.
REQ. 66	Срок на хардуерната гаранция: минимум 3 (три) години.

4. Допълнителни изисквания:

- 4.1. Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или негово официално представителство за правото на разпространение/доставка и предоставяне на гаранционна поддръжка на предлаганите софтуерни и хардуерни продукти на територията на Република България.
- 4.2. При доставка на софтуерното и хардуерното решение трябва да е осигурена последната актуална версия на софтуерните продукти към датата на доставката.
- 4.3. Хардуерната и софтуерната поддръжката следва да е осигурена от производителя и достъпна по Интернет или телефон, като осигури следните параметри:
- Актуализации на програмите, фиксове (поправки) и предизвестия за информационна сигурност;
 - Програмни кодове за обновяване;
 - Основни продуктови и технологични версии, което включва версии, свързани с общата поддръжка, подобрани версии, свързани с поддръжане на функционалността и актуализации на документи;
 - Съдействие при подаване на заявки за техническа помощ за периода на поддръжката;
 - Достъп до web базирана система, включително и възможност за подаване на заявки за техническа помощ чрез Интернет;
 - Право на ъпгрейд на продуктите, което включва получаването на нови версии на софтуера, релийзи за поддръжка и софтуерни пачове, с цел да се осигури стабилност, предсказуемост и подобряване на сигурността, чрез елиминирането на известните проблеми;

5. Място на изпълнение

Място на изпълнение: гр. София, ул. „Елисавета Багряна“ № 20 и ул. „Лъчезар Станчев“ № 11.

6. Изисквания към мрежовата и информационната сигурност²

6.1 Изпълнителят следва да осигури прилагането на изискванията на Закона за електронното управление, Закона за защита на личните данни, Закона за киберсигурност и подзаконовите нормативни актове към тях.

6.2 Във връзка с мрежовата и информационната сигурност на Бенефициера (АВ) и в съответствие с чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:

(а) Гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на Услугата (в т.ч. подизпълнители, когато е приложимо) и които ще имат достъп до информация и активи, при взаимодействието им със служители на Бенефициера (АВ), ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.

(б) При предоставяне на Услугата спазва правилата за сигурността на информацията на Бенефициера (АВ). За целта, непосредствено преди началото на изпълнение, ангажираните от Изпълнителя за предоставяне на Услугата лица (в т.ч. и подизпълнителите, когато е приложимо), които ще имат достъп до информация и активи на Бенефициера (АВ), подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Бенефициера (АВ). При промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до два работни дни от промяната.

(в) определя компетентното лице, отговорно за мрежовата и информационна сигурност, което осъществява взаимодействие с компетентно лице от страна на Бенефициера (АВ) при възникване на инцидент по МИС.

(г) осигурява адекватни и комплексни мерки за защита за мрежова и информационна сигурност, основани на извършения анализ и оценка на риска, с цел да се гарантира необходимото ниво на сигурност. Имплементираните смекчаващи механизми трябва да са пропорционални на рисковете, в частност на щетите, които те биха могли да нанесат.

6.3 Изпълнителят се задължава да не разпространява информация, станала му известна при и по повод изпълнението на Услугата на трети страни без изричното писмено съгласие на Бенефициера (АВ).

6.4 Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Заявката („лица по чл. 10, ал. 2 от НМИМИС“) имат следните права и задължения:

(а) При изпълнението на задълженията си, осъществяват комуникация с лицата, които ще имат достъп до системите на съответната администрация;

(б) Лицето по чл. 10, ал. 2 от НМИМИС от страна на Изпълнителя отговаря за прилагането на адекватни мерки за мрежова и информационна сигурност от страна на Изпълнителя (и на подизпълнителите, когато е приложимо);

(в) При получена информация, лица по чл. 10, ал. 2 от НМИМИС осъществяват незабавна комуникация по телефон и/или имейл и предприемат действия за извършване на анализ на: причините за влошаване на качеството по отношение на времената за реакция и за възстановяването на работата; условията, при които инцидентът може да бъде затворен; рискът за постигане на целите на мрежовата и информационната сигурност на Бенефициера (АВ);

(г) При констатирано неспазване на изискванията за сигурност на информацията или неспазване на договорените срокове, количество и/или качество на услугата, което може

² Изискванията към мрежовата и информационната сигурност са приложими, в случай, че по време на изпълнение на заявката Изпълнителят (подизпълнителите, когато е приложимо) имат достъп до информация и активи на Бенефициера (АВ), които са предмет на защита съгласно приложимото законодателство в областта.

да създаде риск за мрежовата и информационната сигурност за Бенефициера (АВ), лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на съответната администрация от страна на Бенефициера (АВ) и на Изпълнителя извършват анализ и набеязват мерки за отстраняване на допуснатата нередност в определен срок.