

Приложение № 2
към рамков договор ИС-28/02.10.2023 г.

ЗАЯВКА по Рамков договор № ИС-28/02.10.2023 г. (ПО-16-2803/02.10.2023 г. на ИО АД)		☒
ЗАЯВКА по Рамков договор № ИС-28/02.10.2023 г. (ПО-16-2803/02.10.2023 г. на ИО АД) (актуализирана)		☐ ¹
Позиция от ПГ-2026 г.:	<i>№ по ред от ПГ</i>	19
Описание на проект съгласно ПГ:	<i>Осигуряване на мрежово оборудване за изнесени работни места на АГКК (2 бр. защитна стена)</i>	
CPV код	32522000	
Рег. номер на писмо от МИДТ за утвърждаване на проекта /становище по проекта	<i>МИДТ Рег.№ 90-03-572/30.09.2026</i>	
Изискване за достъп до класифицирана информация ДА/НЕ	НЕ	
Стойност: <i>(стойността следва да съответства на заложената в План-графика) без ДДС, в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово</i>		5 350,00 евро без ДДС
Начин за плащане: <i>(еднократно, на части, периодически, авансово или др.)</i>		<i>Еднократно, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане дейностите по осигуряване на мрежовото оборудване и издадена фактура</i>
Плащане с акредитив или авансово ДА/НЕ		НЕ
Документи за плащане с акредитив или авансово		<i>Неприложимо</i>
Срок на изпълнение: <i>(от дата – до дата или в месеци, ако не е обвързан с конкретна дата)</i>		<i>Срок за осигуряване – до 4 месеца от датата на подписване на заявката; Срок на валидност на поддръжката – 36 месеца от датата на осигуряване</i>
Гаранционен срок: <i>(от дата – до дата или в месеци, ако не е обвързан с конкретна дата)</i>		<i>Неприложимо</i>
Отчитане: <i>(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)</i>		<i>Еднократно, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане дейностите по осигуряване на мрежовото оборудване</i>
Приложения: <i>(напр: технически параметри, образци на отчетни документи)</i>		<i>Технически параметри</i>
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		

¹ Отбелязва се в случай че заявката е актуализирана

ЗАЯВКАТА е ИЗГОТВЕНА ОТ:		
Ръководител на проект по заявката от страна на БЕНЕФИЦИЕРА (напр: представител на дирекцията – Заявител):		Подпис:
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:		Подпис:
Ръководител на договора от страна на БЕНЕФИЦИЕРА:		Подпис:
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Ръководител на проект по заявката		Подпис:
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		Подпис:

***Забележка:** С една заявка могат да се възлагат повече от един проект по ПГ, само когато те са еднотипни и управлението им (възлагане, изпълнение, отчитане) може да се извършва съгласно описаните 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.*

ТЕХНИЧЕСКИ ПАРАМЕТРИ

„Осигуряване на мрежово оборудване за изнесени работни места на АГКК (2 бр. защитна стена)“

Гр. София, 2026 г.

I. ПРЕДМЕТ

Предметът на заявката включва осигуряването на мрежово оборудване за изнесени работни места на АГКК (2 бр. защитна стена)

II. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

Спецификация – минимални изисквания	
REQ.1	Количество – 2 броя.
REQ.2	Устройствата следва да бъдат конфигурирани и да работят в режим основно и резервно (spare). При отказ на основното резервното трябва да бъде лицензирано и приведено в работа среда в срок до 12 часа
REQ.3	Изграждане на сектори с различна степен на доверие, които да разделят мрежата на отделни сегменти и прилагане на политики на база потребителски имена от Активната Директория;
REQ.4	Системата да анализира съдържанието за наличие на зловреден код като включва минимум AntiVirus, AntiSpyware, IPS;
REQ.5	AntiVirus инспекцията да може да задържа Zero day файл в защитната стена докато получи отговор за неговата репутация.
REQ.6	Системата за анализ на Zero Day зловреден код трябва да използва минимум следните методи за анализ: Static Analysis, Machine Learning, Dynamic Analysis;
REQ.7	Системата да анализира PE, ELF файлове PowerShell скриптове в защитната стена и предоставя защита в реално време;
REQ.8	Системата следва да инспектира за заплахи HTTPS и HTTP 2.0 протокола чрез декриптиране;
REQ.9	Решението да може да изпраща декриптирани потоци от данни към трети страни за допълнителен анализ.
REQ.10	Решението да може да дистрибутира входящите NAT сесии между няколко адреса като използва минимум следните методи : Round Robin, Source IP Hash, Least Sessions
REQ.11	Филтриране на уеб сайтовете по клиентски категории и ограничаване на достъпа до опасно съдържание в Интернет;
REQ.12	Системата да анализира URL и тяхното съдържание в реално време. Всяка заявка за достъп да бъде анализирана чрез Machine Learning на база на HTTP Request;
REQ.13	Системата за IPS да използва машинно, задълбочено обучение да открива и блокира непознати Command and Control (C2), при преминаване на непознат HTTP, HTTP2, SSL, TCP и UDP трафика през защитната стена;
REQ.14	Управлението на устройството трябва да се реализира чрез физически отделени процесор и памет отделени от ресурсите използвани за управление на трафика;
REQ.15	Операционната система на устройството да позволява на администратора да работи върху копие на работещата конфигурация и след като е готов с промените при потвърждение да се извърши валидация, резервно копие (backup) и прилагане на промените.
REQ.16	Администратора трябва да може да изисква прекатегоризация на даден URL директно от графични интерфейс на защитната стена;
REQ.17	Решението да използва защитната стена, за да анализира и открива phishing чрез ML анализ на изображения и домейни, CAPTCHA интегриран анализ,

	превенция на кражба на идентификационни данни (Username / password) в реално време
REQ.18	Наличие на DLP (Data Loss Prevention) функционалност, за ограничаване на движението на конфиденциални файлове към и извън организацията;
REQ.19	Политиката за декриптиране трябва да има възможност да се настройва на база на URL или URL категория;
REQ.20	Решението да притежава възможност да ограничава достъпа на потребителите до Web сървъри, които не поддържат минимални изисквания за валиден публичен сертификат и съответно високо ниво на сигурност (TLSv1.1, TLSv1.2, TLSv1.3);
REQ.21	Предложеното решение за защитна стена от следващо поколение трябва да поддържа IKEv2 VPN мрежи, устойчиви на квантови атаки (Quantum-Resistant - QR).
REQ.22	Защитата от квантови атаки трябва да съответства на минимум: RFC 8784, RFC 9242 и RFC 9370 с цел смекчаване на риска от атаки тип „Събери сега, декриптирай по-късно“.
REQ.23	Предложеното решение за защитна стена от следващо поколение трябва да има възможност чрез допълнителен лиценз за управление да предостави цялостна стратегия за пълна, миграция към криптография, устойчива на квантови атаки (PQC) включително видимост върху всички криптографски активи (устройства, системи, приложения) и техните детайли: версии (TLS, SSH, VPN), управление на сертификати, генериране, размери и съхранение на ключове.
REQ.24	Препращане на подозрителните DNS заявки към устройството с цел ограничаване на достъпа и регистриране на заразени машини в мрежата;
REQ.25	Предложението решение трябва може да изгражда отдалечен VPN достъп чрез агент инсталиран на крайно клиентската машина Windows, macOS;
REQ.26	Възможност за QoS трафика според типа приложение потребител и/или URL категория;
REQ.27	Прозрачна идентификация на потребителите от Активната директория без изискване на крайната машина да се инсталира агент, настройки в browser или отваряне на Web Portal;
REQ.28	Да предоставя идентифициране на устройства (Device Fingerprint, IoT) в мрежата на база поведение, мета данни и логове;
REQ.29	Да може при регистрирана атака (log) автоматично да поставя засегнатите потребители и IP в група с ограничен достъп до мрежата (изолация или карантина);
REQ.30	Да предоставя възможност за съставяне на политика за сигурност базирана на устройство независимо от неговия IP Address, локация и потребител;
REQ.31	Решението да може да чете данните в X-Forwarded-For (XFF) за идентифициране на реалния източник на данни (IP Address), когато той се намира зад други мрежови устройства;
REQ.32	Защита на корпоративните потребителски имена и пароли, посредством блокиране или ограничаване на тяхното използване в външни за организацията системи и публично достъпни доставчици (Dropbox, Google, Facebook, LinkedIn);
REQ.33	Решението да включва функционалност позволяваща служебния достъп до публични облачни услуги като Office 365, Google, Dropbox и YouTube, и ограничаваща достъпа до лични потребителски акаунти за същите приложения;
REQ.34	Анализа на логовете и репортинг да се извършва от самото устройство през неговия графичен интерфейс без да е необходима инсталация на допълнителен софтуер;

REQ.35	Решението да притежава Уеб базиран интерфейс с различни статистики на база време, приложение, категории, потребители, заплахи и други;
REQ.36	Генерираните отчети и логове следва да са обогатени с данни за потребител и група, получена от интеграция с бази за управление на потребителите (Active Directory, LDAP и други);
REQ.37	Решението да може автоматично да тегли IP, Domain или URL листи от Web Server собственост на Възложителя или външна организация с цел ограничаване / позволяване на достъпа до горе споменатите;
REQ.38	Решението да може автоматично да открива какви приложения работят в организацията и да предлага лист от такива, които да бъдат добавени към нови или вече съществуващи правила за сигурност;
REQ.39	Решението да предоставя възможност за надграждане чрез лиценз която позволява на защитната стена да изтегля нови приложения от облака за приложения, които нямат конкретни предварително дефинирани сигнатури от производителя
REQ.40	Решението да има механизъм за откриване и превенция на DNS Tunneling канали за комуникация, включително ограничаване достъпа до автоматично генерирани домейни (Domain generation algorithms).
REQ.41	Да открива в реално време атаки като инспектира DNS Response и DNS Request.
REQ.42	DNS защитата да може в реално време без допълнителни модули или платформи да прилага активна защита към специфични техники и категории като: "C&C domains", "DGA detection", "NXNSAttack", "DNS rebinding", "Malware domains", "Newly Registered Domains", "Phishing Domains", "Parked domains", "Proxy avoidance", "Ad tracking domains", "Hijacked Domains", "Misconfiguration Domains".
REQ.43	Системата да открива и управлява IoT (Internet of Things) устройства като предоставя възможност за автоматично генериране на препоръчани правила за достъп и контрол.
REQ.44	Системата да може да пропуска до три софтуерни версии при upgrade като дава възможност да изберете да пропуснете две основни версии и една второстепенна или една основна версия и две второстепенни.
REQ.45	След изтичането на абонаментите решението да продължи да работи с наличните до момента сигнатури за IPS, AntiVirus и разпознаване на приложенията.
REQ.46	Минимална пропускателна способност с активирана функция за идентификация на приложенията - минимално 2.3 Gbps
REQ.47	Минимална пропускателна способност с активирани всички функционалности за защита: IPS / AntiVirus/ AntiMalware / URL / Firewall / Application Control / File blocking - минимално 1.0 Gbps
REQ.48	Минимална производителност за IPsec VPN - минимално 1.0 Gbps
REQ.49	Минимален брой TCP сесии - 190 000
REQ.50	Минимален брой нови сесии в секунда - 32 000
REQ.51	Разпознати и поддържани приложения (минимум) - 5200
REQ.52	Да разполага с: 8 x 1Gbps Base-T интерфейса
REQ.53	Режим на работа на интерфейсите - L2, L3, Tap, Transparent едновременно/микс да се използват върху едно устройство.
REQ.54	Машрутизиращи протоколи - OSPFv2/v3, BGP with graceful restart, RIP, static routing Policy-based forwarding Point-to-Point Protocol over Ethernet (PPPoE)
REQ.55	Минимални изисквания към IPsec имплементация - да поддържа Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate authentication) ; Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512

REQ.56	Минимален брой конкурентни SSL VPN потребителя включени в системата (постоянни лицензи) - 800 SSL VPN потребителя
REQ.57	Минимален брой IPSec Site-to-Site VPN - 1000
REQ.58	Устройството да поддържа виртуални таблици за маршрутизация минимум 2 броя
REQ.59	Всички конфигурации за интерфейсите модули на защитната стена трябва да поддържат IPv6 както и всички контролни функции на системата трябва да се налични и за IPv6
REQ.60	Системата следва да декриптира и инспектира SSL като поддържа : TLS v1.1, TLS v1.2, TLS v1.3
REQ.61	Всяко от устройствата в системата да има възможност да се управлява посредством имплементация на REST based API, извличане на данни и репорти в XML формати. Всяко от устройствата в системата следва да поддържа всеки един от следните методи за управление: CLI, уеб конзола, централизирана система за управление
REQ.62	Минимален брой интерфейси за управление - 1 x 100/1000 out-of-band management port; 1 x RJ-45 конзолен порт; 1 x Micro USB
REQ.63	Предназначена за вграждане в 19“ шкаф с максимален размер 1U
REQ.64	Резервирано захранване и входно напрежение (Входяща честота) 100-240VAC (50-60Hz)
Гаранция и поддръжка:	
REQ.65	Софтуерна и хардуерна гаранционна поддръжка в режим 365x24x7
REQ.66	Софтуерна и хардуерна гаранционна поддръжка минимално 36 месеца
REQ.67	Участника следва да използва необходимите лицензи за гаранционна поддръжка от Производителя. Доказва се чрез посочване на партиден номер.

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизиран от производителя или официален негов представител за право на разпространение/доставка на предлаганите продукти на територията на Република България

III. СРОК НА ИЗПЪЛНЕНИЕ

Срок на осигуряване на мрежовото оборудване – до 4 месеца от подписване на заявката.

Срок на софтуерната и хардуерната гаранционна поддръжка е 36 месеца, от датата на осигуряване.

IV. МЯСТО НА ДОСТАВКА И ГАРАНЦИОННО ОБСЛУЖВАНЕ

Административната сграда на Агенция за геодезия, картография и кадастър, с адрес: гр. София 1618, ул. „Мусала“ № 1.

V. ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ²

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 Възложителя/ Бенефициера/АГКК/МИДТ, които са предмет на защита съгласно приложимото законодателство в областта.

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.
2. Във връзка с мрежовата и информационната сигурност на Бенефициера/Възложителя/АГКК/МИДТ 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/Възложителя/АГКК/МИДТ 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/Възложителя/АГКК/МИДТ. 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/Възложителя/АГКК/МИДТ, подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Бенефициера/Възложителя/АГКК/МИДТ. 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 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.
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/Възложителя/АГКК/МИДТ.
4. При неспазване на изискванията за сигурност на информацията Изпълнителят дължи неустойка съгласно уговореното в договора.
5. Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Договора („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 Бенефициера/Възложителя/АГКК/МИДТ;
 - (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/Възложителя/АГКК/МИДТ;
- (г) При констатирано неспазване на изискванията за сигурност на информацията или неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за мрежовата и информационната сигурност за Бенефициера/Възложителя/АГКК/МИДТ, лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на АГКК от страна на Бенефициера/Възложителя/АГКК/МИДТ и на Изпълнителя извършват анализ и набеязват мерки за отстраняване на допуснатата нередност в определен срок.