Приложение № 2
към рамков договор № 15/05.08.2025 г.

ЗАЯВКА по Рамков договор № ДОГ-00-160/21.10.2025 г. **(№ ПО-16-2761/04.11.2025 на ИО АД)**	☒
ЗАЯВКА по Рамков договор № № ДОГ-00-160/21.10.2025 г. **(актуализирана)**	☐ [1]

Позиция от ПГ-2025 г.:	*№ по ред от ПГ*	*6*
Описание на проект съгласно ПГ:	*Доставка на защитни стени*	
CPV код	*32420000-3*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*№ МЕУ- 19953/23.12.2025*	
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*	***105 600,00 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 доставка на защитни стени* *В случай на невъзможност за изпълнение на дейностите до края на бюджетната година - авансово плащане през м. декември 2025 г., срещу предоставена от Изпълнителя гаранция, обезпечаваща 100% стойността на авансовото плащане с вкл. ДДС и издадена фактура.*
Плащане с акредитив ДА/НЕ	*Да* *В случай на невъзможност за изпълнение на дейностите до края на бюджетната година - авансово плащане през м. декември 2025 г., срещу предоставена от Изпълнителя гаранция, обезпечаваща 100% стойността на авансовото плащане с вкл. ДДС и издадена фактура.*
Документи за плащане с акредитив	*Не е приложимо.*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата*)	*До 4 месеца след подписване на заявката.*
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата*)	*Съгласно техническите параметри.*
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*Еднократно, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ доставка на защитни стени*
Приложения: (*напр: технически*	*Технически параметри.*

[1] Отбелязва се в случай че заявката е актуализирана

*параметри, образци на отчетни документи***)**		
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):		*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:*

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА

ДОСТАВКА НА ЗАЩИТНИ СТЕНИ

1. ПРЕДМЕТ

В предмета на заявката се включва доставка на 27 броя защитни стени за нуждите на Държавна Агенция архиви.

2. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

2.1 Дейност 1 :

Минималните изискванията на Бенефициера относно обхвата и изпълнението на дейностите по доставка на 27 броя защитни стени за нуждите на Държавна Агенция архиви са, както следва :

	Минимални изисквания
REQ.1.	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.2.	Системата да анализира съдържанието за наличие на зловреден код като включва минимум AntiVirus, AntiSpyware, IPS;
REQ.3.	AntiVirus инспекцията да може да задържа Zero day файл в защитната стена докато получи отговор за неговата репутация.
REQ.4.	Системата да анализира непознати заплахи (Zero Day зловреден код) в защитена среда като създава и дистрибутира сигнатури в реално време.
REQ.5.	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.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 протокола чрез декриптиране;
REQ.9.	Системата следва да инспектира за заплахи HTTP 1.1 и HTTP 2.0 протоколи;
REQ.10.	Да филтрира уеб сайтовете по категории и ограничаване на достъпа до опасно съдържание в Интернет, включително мултикатегоризация на URL съгласно тип на съдържанието и риск;
REQ.11.	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.12.	Управлението на устройството трябва да се реализира чрез физически отделени процесор, памет и интерфейси отделени от ресурсите използвани за управление на трафика.
REQ.13.	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.14.	Решението да може да дистрибутира входящите NAT сесии между няколко адреса като използва минимум следните методи: Round Robin, Source IP Hash, Least Sessions
REQ.15.	Администратора трябва да може да изисква прекатегоризация на даден URL директно от графични интерфейс на защитната стена.
REQ.16.	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.17.	Наличие на DLP (Data Loss Prevention) функционалност, за ограничаване на движението на конфиденциални файлове.
REQ.18.	Политиката за декриптиране трябва да има възможност да се настройва на база на URL или URL категория;
REQ.19.	Решението да притежава възможност да ограничава достъпа на потребителите до Web сървъри, които не поддържа минимални изисквания за валиден публичен сертификат и съответно високо ниво на сигурност (TLSv1.1, TLSv1.2, TLSv1.3);
REQ.20.	Предложението решение трябва може да изгражда отдалечен VPN достъп чрез агент инсталиран на крайно клиентската машина с Windows и MacOS .
REQ.21.	Агента за VPN достъп трябва да поддържа (да може да бъде инсталиран) чрез добавяне на допълнителен лиценз на минимум следните операционни системи: Android, iOS, Raspbian, Ubuntu.
REQ.22.	Възможност за QoS трафика според типа приложение потребител и/или URL категория.
REQ.23.	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.24.	Да предоставя възможност за надграждане с допълнителен лиценз за идентифициране на устройства (Device Fingerprint) в мрежата на база поведение, мета данни и логове. За карантина на заразени устройства независимо от техните IP адреси, локация и потребител.
REQ.25.	Да може при регистрирана атака (log) автоматично да поставя засегнатите потребители и IP в група с ограничен достъп до мрежата (изолация или карантина).
REQ.26.	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.27.	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.28.	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.29.	Решението да притежава Уеб базиран интерфейс с различни статистики на база време, приложение, категории, потребители, заплахи. Анализа на логовете и репортинг да се извършва от самото устройство чрез неговия

	графичен интерфейс без да необходима инсталация на допълнителен софтуер.
REQ.30.	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.31.	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.32.	Да открива в реално време атаки като инспектира DNS Response и DNS Request.
REQ.33.	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.34.	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.35.	Решението да притежава облачна услуга за събиране и анализ на служебни данни от устройството като чрез машинно обучение препоръчва добри практики и открива аномалии в нормалната работа.
REQ.36.	Да има възможност за надграждане чрез лиценз за услуга която позволява на защитната стена да категоризира непознати приложения в облака на производителя за които няма конкретни предварително дефинирани сигнатури.
REQ.37.	Решението да предоставя възможност за надграждане чрез лиценз за защита на крайно клиентските машини, позволяващ събиране и анализ на всички логове (от крайните точки и защитните стени) в защитена облачна среда на производителя.
REQ.38.	Системата да има възможност за надграждане с допълнителен лиценз инсталиран на защитната стена, с който да открива и управлява IoT (Internet of Things) устройства като предоставя възможност за автоматично генериране на препоръчани правила за достъп и контрол.
REQ.39.	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.

	Параметър	**Минимално изискване**
REQ.40.	Минимална пропускателна способност с активирана функция за идентификация на приложенията (HTTP трафик)	2.5 Gbps
REQ.41.	Минимална пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/ AntiSpyware / URL / Firewall / Application Control / Sandbox	1.1 Gbps
REQ.42.	Минимална производителност за IPsec VPN	1.1 Gbps
REQ.43.	Минимален брой TCP сесии	200 000
REQ.44.	Минимален брой нови сесии в секунда	30 000

REQ.45.	Разпознати и поддържани приложения (минимум)	5 000
REQ.46.	Минимален брой мрежови интерфейси	Да разполага с 8x10/100/1000 Base-T ports
REQ.47.	Режими на работа на интерфейсите	L2, L3, Tap, Transparent едновременно/микс да се използват върху едно устройство.
REQ.48.	Машрутизиращи протоколи	OSPFv2/v3, BGP with graceful restart, RIP, static routing Policy-based forwarding Point-to-Point Protocol over Ethernet (PPPoE)
REQ.49.	Минимални изисквания към IPSec имплементация	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.50.	Минимален брой конкурентни SSL VPN потребителя включени в системата (постоянни лицензи)	100 SSL VPN потребителя
REQ.51.	Минимален брой IPSec SD-WAN Site-to-Site VPN	30 отдалечени точки
REQ.52.	Устройството да поддържа виртуални таблици за маршрутизация минимум	2 броя
REQ.53.	IPv6 поддръжка	Всички конфигурации за интерфейсните модули на защитната стена трябва да поддържат IPv6 както и всички контролни функции на системата трябва да се налични и за IPv6
REQ.54.	Инспекция на SSL криптиран трафик, без оглед на прилежащия протокол, като предоставя декриптирания трафик на всички свои функционални компоненти, за инспекция и налагане на политики над съдържанието	Системата следва да декриптира и инспектира SSL като поддържа : TLS v1.1, TLS v1.2, TLS v1.3
REQ.55.	Управление на устройството	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.56.	Режим на надеждност	Active-Passive, Active/Active
REQ.57.	Минимален брой интерфейси за управление	1 x RJ45 (1GB) порт за управление 1 x RJ-45 конзолен порт

		1 x USB port 1 x Micro USB port
REQ.58.	Монтаж, размери, охлаждане	Предназначена за вграждане в 19‘‘
REQ.59.	Захранване и входно напрежение (Входяща честота)	Външно, с максимална консумирана мощност не повече от 35W
REQ.60.	Софтуерна и хардуерна гаранционна поддръжка тип 365x24x7	минимум 12 месеца от производителя,

Всички лицензи и права за ползване, осигурени чрез изпълнението на настоящата заявка, следва да са на името на ДА архиви. Изпълнителят предоставя на ДА архиви пълната информация относно осигурената осигурените лицензи - всички лицензни файлове, ключове, активационни кодове, данни за достъп до официални сайтове на производителите на софтуерните продукти, когато това е приложимо

3. МЯСТО НА ДОСТАВКА И ГАРАНЦИОННО ОБСЛУЖВАНЕ

3.1 Мястото на доставка е сградата на ДА архиви , в гр. София, ул. „Московска“ №5

3. 2. Услугите по техническа поддръжка се предоставят отдалечено, при необходимост от оказване на съдействие на място - ДА архиви , в гр. София, ул. „Московска“

4. ДОПЪЛНИТЕЛНИ ИЗИСКВАНИЯ :

Доставените продукти по следва да са нови, неупотребявани, нерециклирани към датата на доставка.

Изпълнителят следва да осигури изпълнението на доставките от лице, надлежно оторизирано от производителя или от официален негов представител с права за извършване на продажба на територията на Република България, като предостави копие на документа, удостоверяващ оторизацията, придружено от превод на български език.

5. ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ[2]

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 Възложителя/Бенефициера (МЕУ/ДАА) и в съответствие с чл. 10 от Наредбата за

[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 (МЕУ/ДАА), които са предмет на защита съгласно приложимото законодателство в областта.

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 Възложителя/Бенефициера (МЕУ/ ДАА), 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 Възложителя/Бенефициера (МЕУ/ ДАА). 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 Възложителя/Бенефициера (МЕУ/ ДАА), подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Възложителя/Бенефициера (МЕУ/ ДАА). 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 Възложителя/Бенефициера (МЕУ/ ДАА) 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 Възложителя/Бенефициера (МЕУ/ ДАА).

4. 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 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 Възложителя/Бенефициера (МЕУ/ ДАА);

(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 Възложителя/Бенефициера (МЕУ/ ДАА лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на съответната администрация от страна на Възложителя/Бенефициера (МЕУ/ ДАА) и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.