Приложение № 2
към рамков договор № 67/24.10.2024 г.

ЗАЯВКА по Рамков договор № 67/24.10.2024 г. (№ ПО-16-3173/24.10.2024 г. на „Информационно обслужване“ АД)	☒
ЗАЯВКА по Рамков договор № 67/24.10.2024 г. (№ ПО-16-3173/24.10.2024 г. на „Информационно обслужване“ АД) (актуализирана)	☐ [1]

Позиция от ПГ-2025 г.:	*№ по ред от ПГ*	*12*
Описание на проект съгласно ПГ:	*Доставка на защитни стени втори слой*	
CPV код	*32420000-3*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*МЕУ-9060/23.06.2025 г.*	
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*	*137 100.00 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 осигуряването на софтуер за резервни копия*
Плащане с акредитив или авансово ДА/НЕ	*НЕ*
Документи за плащане с акредитив или авансово	*НЕ*
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***)**	*Неприложимо*
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 осигуряването на софтуер за резервни копия*
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):		*Подпис:*

ЗАЯВКАТА е ОДОБРЕНА ОТ:

Координатор на договора от страна на	.	*Подпис:*

[1] Отбелязва се в случай че заявката е актуализирана

ВЪЗЛОЖИТЕЛЯ:	
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.*

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

ПРИЛОЖЕНИЕ № 1

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА:

„Доставка на защитни стени втори слой за нуждите на Министерството на енергетиката“

Гр. София 2025 г.

I. ПРЕДМЕТ

В предмета на заявката се включва доставка на защитни стени втори слой за нуждите на Министерство на енергетиката.

II. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

Изискванията на Бенефициера относно обхвата и изпълнението на дейностите по доставка на защитни стени втори слой за МЕ са, както следва:

Опорни защитни стени от следващо поколение за защита на сървърни компоненти

Спецификация – минимални изисквания	
REQ.1	Количество – 2 броя
REQ.2	Тип на кутията/шасито - за директен монтаж в 19“ шкаф.
REQ.3	Захранване – резервирано, по схема 1:1 с минимум два токозахранващи модула работещи в диапазона 220-240v AC, 50Hz.
REQ.4	Работен температурен диапазон от 0° до +40 °C.
REQ.5	Работна относителна влажност от 10% до 85%.
REQ.6	Минимум 8 100/1000Base-T интерфейса 8 броя 1/10GE SFP+ интерфейса.
REQ.7	Брой USB портове - минимум 1 брой.
REQ.8	Ethernet порт за управление - минимум 1 брой.
REQ.9	Сериен конзолен порт - минимум 1 брой.
REQ.10	Възможност за добавяне на минимум 8 броя 1/10GE SFP+ интерфейса.
REQ.11	Производителност: • минимум 10 Gbps със работещи statefull inspection firewall, IPS и deep packet inspection. • брой сесии – минимум 1 500 000. • нови сесии за 1 секунда - минимум 90 000. • IPSec производителност – минимум 5 Gbps. • Производителност на TLS декриптиране – минимум 3 Gbps
REQ.12	Да поддържа прозрачен режим на работа – Inline.
REQ.13	Да поддържа режим на работа като маршрутизатор.
REQ.14	Да поддържа IPSec тунели с IKE/IKEv2 управление на сесиите и следните методи за защита: • Encryption: 3DES, AES-128 и AES-256. • Authentication: preshared key, RSA и ECDSA. • Integrity: SHA, SHA-256, SHA-384, SHA-512.
REQ.15	Да поддържа SCEP протокол за получаване на сертификат.
REQ.16	Да поддържа OCSP за проверка валидността на сертификати.
REQ.17	Да поддържа декриптиране на трафик за инспекция.
REQ.18	Да поддържа SSL VPN за минимум 2000 потребителя.
REQ.19	Да се поддържа SSL клиент за връзка към защитната стена за следните операционни системи: • Windows 11/10/8 • macOS 12/11/10 • Red Hat, Ubuntu и SUSE Linux дистрибуции.
REQ.20	Да поддържа 802.1Q VLAN.
REQ.21	Да има вградена IPS система.
REQ.22	Да има вградена Anti-Malware система за защита от файлове със зловреден код.

REQ.23	Да поддържа ретроспективно уведомяване на администратора при получаване на нова информация, която класифицира вече свалени файлове като съдържащи зловреден код.
REQ.24	Да поддържа категоризация на Web URL на база категории и ниво на риска.
REQ.25	Да има вградена DPI система с класифициране на мрежовия трафик на ниво приложения и категории от приложения.
REQ.26	Да поддържа минимум следните протоколи за маршрутизация: • RIP и RIPv2 • OSPFv2 и OSPFv3 • BGPv4
REQ.27	Да поддържа минимум IGMPv2 и PIM-SM мултикаст маршрутизиране.
REQ.28	Да поддържа динамичен и статичен NAT.
REQ.29	Да поддържа динамичен и статичен PAT.
REQ.30	Да поддържа минимум следните PAT и NAT услуги: • NAT за IPv4 • NAT 66 • NAT 64/46 транслации
REQ.31	Да поддържа NAT AGL за SIP, H.323 и FTP протоколи.
REQ.32	Да позволява обособяване на DMZ зони.
REQ.33	Да поддържа rate limiting с класифициране на трафика на база минимум следните параметри: • Интерфейс • IP мрежи • Приложения и категории от приложения • URL категория и репутация • Active Directory потребители и групи от потребители
REQ.34	Възможност за добавяне на интеграция с Microsoft Active Directory за идентификация на потребителите и създаването на Firewall политики на база AD групи и потребителите.
REQ.35	Да поддържа идентификация на потребителите чрез външен RADIUS сървър.
REQ.36	Да поддържа active-standby HA режим на работа.
REQ.37	Да поддържа минимум следните методи за управление и наблюдение: • Конзола, HTTP и HTTPS. • Ping • DNS • NTP • SSHv2c и SNMPv3 • Syslog • Експортиране на трафична информация чрез IPFIX, Netflow, Jflow или подобен протокол към външна система за трафичен анализ. • Идентификация на администратрите чрез локална база, RADIUS сървър и LDAP. • Отделен Ethernet порт за out of band управление и наблюдение на устройството.
REQ.38	Устройството да има инсталирана и лицензирана с постоянен лиценз операционна система.
REQ.39	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя.
Гаранция и поддръжка:	
REQ.40	Хардуерна гаранция за срок от минимум 3 (три) години.
REQ.41	Техническа поддръжка за срок от минимум 3 (три) години.
REQ.42	Получаване на нови версии на софтуера за срок от минимум 3 (три) години.
REQ.43	Лицензни абонаменти за използване на софтуерни функции за срок от минимум 3 (три) години.

Система за управление и наблюдение на защитни стени (NGFW) – 1 брой

Спецификация – минимални изисквания	
REQ.1	Капацитет – управление на минимум 2 NGFW системи
REQ.2	Да поддържа пълно управление и наблюдение на предложените опорни NGFW системи в настоящата техническа спецификация.
REQ.3	Да поддържа корелация на събитията получавани от NGFW до инциденти.
REQ.4	Да поддържа създаване и прилагане на NGFW политики върху управляваните устройства.
REQ.5	Да поддържа автоматично прилагане на политики при определени събития в NGFW.
REQ.6	Да поддържа дългосрочно съхранение на събитията.
REQ.7	Да поддържа автоматично изпълнение на предварително планирани задачи.
REQ.8	Да поддържа интеграция с Active Directory.
REQ.9	Да поддържа идентификация на потребители и администратори чрез външен RADIUS сървър.
REQ.10	Да има GUI WEB интерфейс.
REQ.11	Да поддържа разделяне на управление и наблюдение на множество под организации – multitenant възможности.
REQ.12	Да поддържа обмяна на контекстна информация и интеграция с външни системи през API.
REQ.13	Да визуализира различни събития, инциденти и тенденции свързани със сигурността в управляваните NGFW.
REQ.14	Да позволява създаването на доклади чрез управляеми дашборди.
REQ.15	Да визуализира трафична информация на ниво приложения.
REQ.16	Инсталация върху виртуални, хардуерни аплайънси или сървъри, съгласно изискванията на производителя.
REQ.17	Ако предложението на участник включва сървъри, то те трябва да се доставят с всички необходими лицензи за операционни системи, бази данни и допълнителен софтуер, съгласно изискванията на производителя.
REQ.18	Виртуалните аплайънси трябва да са съвместими с VMWare ESXi инфраструктура.
Гаранция и поддръжка:	
REQ.19	Техническа поддръжка за срок от минимум 3 (три) години.
REQ.20	Получаване на нови версии на софтуера за срок от минимум 3 (три) години.
REQ.21	Лицензни абонаменти за използване на софтуерни функции за срок от минимум 3 (три) години.

Всички лицензи и права за ползване, осигурени чрез изпълнението на настоящата заявка, следва да са на името на МЕ. Изпълнителят предоставя на МЕ 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

III. СРОК НА ИЗПЪЛНЕНИЕ.

1. Срокът на доставката е до 4 месеца след подписване на заявката.

2. Срок на хардуерна гаранция е 36 месеца, периодът на изпълнение на услугите по техническа поддръжка е 36 месеца, считано от датата на осигуряване.

IV. МЯСТО НА ДОСТАВКА И ГАРАНЦИОННО ОБСЛУЖВАНЕ

1. Мястото на доставка е сградата на Министерство на енергетиката, в гр. София, ул. Триадица № 8
2. Услугите по техническа поддръжка се предоставят отдалечено, при необходимост от оказване на съдействие на място - сградата на Министерство на енергетиката, в гр. София, ул. Триадица № 8

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

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:

---

[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/МЕ), които са предмет на защита съгласно приложимото законодателство в областта.

(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/МЕ);

(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/МЕ), 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/МЕ) и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.