МИНИСТЕРСТВО НА ИКОНОМИКАТА И ЕНЕРГЕТИКАТА

Д О К У М Е Н Т А Ц И Я

ЗА

УЧАСТИЕ В ПУБЛИЧНА ПОКАНА ЗА ВЪЗЛАГАНЕ НА

ОБЩЕСТВЕНА ПОРЪЧКА С ПРЕДМЕТ:

„Доставка на защитна стена за нуждите на Министерство на икономиката и енергетиката”

София, 2013 г.

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

Надяваме се, че настоящата документация и приложенията към нея ще ви помогнат да се запознаете с условията и да подготвите своите предложения за участие в тази процедура по реда на Глава осма «а» от Закона за обществените поръчки. За всички неуредени в настоящата документация за участие въпроси се прилагат правилата на Закона за обществените поръчки. За всички неуредени въпроси във връзка със сключването, изпълнението и прекратяването на договорите по настоящата обществена поръчка се прилагат разпоредбите на Търговския закон и на Закона за задълженията и договорите.

Документацията за участие в процедурата е безплатна и до нея е предоставен пълен достъп по електронен път от датата на публикуването на публичната покана на Интернет страницата на МИЕ - http://www.mi.government.bg/, рубрика "Обяви и търгове".

Участниците в процедурата, следва да прегледат и да се съобразят с всички указания, образци, условия и изисквания, посочени в Документацията.

Офертите на участниците се приемат всеки работен ден до 17:30 часа, в срок до крайната дата за приемане на офертите, посочена в публичната покана, включително.

За допълнителна информация и въпроси можете да се обръщате към Министерство на икономиката и енергетиката на следните телефони:

02/940 7483 – Ния Панайотова – дирекция «Информационно и комуникационно осигуряване»;

02/940 7563 – Теодор Михайлов – дирекция «Правна»;

02/940 7693 – Цецка Томова – дирекция «Правна».

Правно основание за провеждане на процедурата, предмет на публичната покана, прогнозна стойност и срок на поръчката, методика за оценка, допустимост на офертите и необходими документи, изисквания към начина на представяне на предложенията, технически спецификации

I. Правно основание за провеждане на процедурата: Чл. 14, ал. 4 и Глава осма „а" от Закона за обществените поръчки.

II. Предмет на публичната покана: „Доставка на защитна стена за нуждите на Министерство на икономиката и енергетиката"

III. Прогнозна стойност на поръчката:
Прогнозната стойност на поръчката е до 50 000 лв. (петдесет хиляди лева), без ДДС.

IV. Методика за оценка: Критерият за оценяване на предложенията е най-ниска цена.

V. Допустимост на офертите и необходими документи:

Допустими са офертите, представени в деловодството на Министерството на икономиката, енергетиката и туризма на ул. „Славянска" № 8, до крайния срок: **17:30 ч. на 01.07.2013 г.** и съдържащи следните необходими документи:

Допустими са офертите, представени в деловодството на Министерството на икономиката и енергетиката на ул. „Славянска” № 8, до крайния срок: до 17.30 ч. на 11-ия работен ден от публикуване на поканата в сайта на МИЕ и на сайта на АОП и съдържащи следните необходими документи:

1. Копие от документа за регистрация или единен идентификационен код съгласно чл. 23 от Закона за търговския регистър, когато участникът е юридическо лице или едноличен търговец; копие от документа за самоличност, когато участникът е физическо лице;

2. Предложение за изпълнение на поръчката, съдържащо данни за лицето, което прави предложението (ЕИК, седалище/адрес на управление, адрес за кореспонденция, телефон, факс, e-mail, банкова сметка, обслужваща банка, имена на представляващия дружеството), съгласно образец на Възложителя – Приложение № 1 към публичната покана;

3. Техническо предложение в съгласие с изискванията на Възложителя – Приложение № 2 към публичната покана

4. Отделен плик с надпис „предлагана цена” (по образец – Приложение № 3 към публичната покана)

5. Декларация относно отсъствие на обстоятелствата по чл. 47, ал. 1, т. 1 от ЗОП, попълнена по образец, съгласно Приложение № 5 към публичната покана;

6. Декларация относно отсъствие на обстоятелства по чл. 47, ал. 5 от ЗОП, попълнена по образец, съгласно Приложение № 6 към публичната покана;

7. Декларация за минимум един изпълнен договор с предмет, сходен с предмета на поръчката, през последните три години (съгласно Приложение № 4 към публичната покана).

8. Сертификат за качество ISO 9001:2008 или еквивалент, издаден от акредитиран сертифициращ орган.

9. Списък на приложените документи.

Когато участникът предвижда участие на подизпълнители, това обстоятелство се декларира, като документите по чл. 56, ал. 1, т. 1, 5, 6 от Закона за обществените поръчки се представят за всеки от тях, а изискванията към тях се прилагат съобразно вида и дела на тяхното участие.

Забележка: **Всички документи следва да бъдат представени в оригинал или заверено с подпис на представляващия и печат на участника копие.**

VI. Изисквания към начина на представяне на предложенията:

- представят се в запечатан, непрозрачен, с ненарушена цялост плик, от участника или от упълномощен от него представител, в деловодството на МИЕ, на адрес: София, ул. „Славянска” № 8;
- върху плика участникът посочва адрес за кореспонденция, телефон и по възможност - факс и електронен адрес, наименованието на предмета на услугата, както и следното предписание: "Да не се отваря преди разглеждане от страна на комисията за оценяване и класиране";

- предложение относно предлаганата цена, без ДДС, приложено в отделен непрозрачен плик, в подписан и подпечатан вид, поставен в плика с офертата;
- при приемане на офертата върху плика се отбелязват поредният номер, датата и часът на получаването и посочените данни се записват във входящ регистър, за което на приносителя се издава документ;
- не се приемат за участие в процедурата и се връщат незабавно на участниците предложения, които са представени след изтичане на крайния срок за получаване или в незапечатан, прозрачен или скъсан плик.

VII. Технически спецификации:

Доставка на 2 бр. устройства за мрежова и информационна защита, всяко от които следва да покрива следните критерии:

Операционна система	Да притежава сигурна операционна система (ОС) позволяваща връщането към предварително определена конфигурация в случай на повреда на устройството.
USB портове	Да има минимум два USB порта за инсталиране на операционната система или запазване и възстановяване на конфигурацията на устройството.
Управление	Да притежава сериен порт използваем за първоначална настройка на устройството и ОС, както и за управление чрез команден ред (CLI).
Контролен панел	Да има панел за управление и настройка на операционната система и IP адресите.
Протоколи и приложения	Интегрирана функционалност за проверка на над 500 протокола и приложения
Поддръжка на NAT	Наличие на "Static" и "Dinamic" преобразуване на мрежови адреси с помощта на ръчно и автоматично генерирани NAT-правила
VLAN и поддръжка	Поддръжка на най-малко 1000 VLAN-а
Линк агрегация	Поддръжка на активна и пасивна агрегация по стандарт IEEE 802.3ad
Вътрешни комуникации	Устройството да притежава функционалност да използва цифрови сертификати, издадени от вътрешен сертификат ауторити за вътрешна комуникация между нейните компоненти, за да се предотврати прихващането на комуникацията между тях.
Идентификация на потребител	Поддръжка на LDAP (Active Directory, Novell eDirectory, LDAP Server), RADIUS, TACACS +, RSA SecurID, X.509 сертификати)
Идентификация на потребител и работни станции	Да има наличие на политика на сигурност за идентифициране на потребители и работни станции при използване на правила за сигурност по прозрачен начин, като се използват различни методи: • Clientless с интеграция на Active Directory • Web портал, който се използва за придобиване на идентичности от неидентифицирани потребители, предоставящ сигурност за крайни точки, които не са част от домейн.
Клъстеризиране	Да притежава висока надеждност и разпределяне на натоварването на две или повече устройства (клъстерни възли). Да разпределя трафика между клъстерите, така че изчислителната мощност на множество машини да може да

	бъде комбинирана, за да се увеличи общата производителност. Ако индивидуално устройство стане недостъпно, всички връзки да се пренасочват към определено резервирано устройство без прекъсване на трафика.
VPN топология	Поддръжка на множество тунели за VPN тип звезда
VPN удостоверяване	Да поддържа минимум следните типове удостоверяване: Парола, RADIUS, TACACS, X.509, SecurID, LDAP
Маршрут-базиран VPN	Поддръжка на номерирани или неномерирани VPN тунели
IKE (Фаза 1) Key Exchange	Да поддържа минимум AES128, AES256, 3DES, DES, CAST
IKE (Фаза 1) Data Integrity	Да поддържа минимум MD5, SHA1, SHA256
IKE (фаза 2) Data Encryption	Да поддържа минимум 3DES, AES128, AES256, DES, CAST, DES-40CP, CAST-40, NULL
IKE (фаза 2) Data Integrity	Да поддържа минимум MD5, SHA1, SHA256
IKE (Ph ASE 1) и IPSec (фаза 2) Дифи-Хелман Групи	Да поддържа минимум Група 1 (768 бита), Група 2 (1024 бита), Група 5 (1536 бита), група 14, (2048 бита)
IKE (Фаза 1) Опции	Да поддържа нормално и агресивен режим
Поддръжка на мобилни устройства	L2TP Поддръжка на iPhone, Windows Mobile
Методи за идентификация за уеб портал	Поддръжка на X. 509 цифрови сертификата
Сигурност при поискване	Поддръжка на мобилни устройства за проверка на сигурността, в съответствие с корпоративната политика за сигурност, преди да позволи достъп до ресурси от вътрешната мрежа
Защитено виртуално работно пространство за достъп на отдалечени клиенти	Поддръжка на виртуален десктоп, защитена виртуална среда, изолирани от мрежата, което дава възможност за защита на данните по време на потребителски сесии. Защитава всички конкретни данни, натрупани от страна на клиента по време на сесията. Да може да криптира и изтрива браузър и кеш приложения, файлове и т.н., когато сесията приключи Поддръжка на блокиране на неоторизиран достъп и прекъсване на достъпа до клипборда вътре в защитената виртуална среда
Мобилни защита на потребителите	Предотвратява атаките от червей и троянски приложения
Мобилни устройства	Да поддържа минимум iPhone 3G/3GS, iPhone 4S, Android 2.1 +, IPAD, Windows XP/Vista/7
Уеб портал - уеб браузър клиентска	Да поддържа минимум Internet Explorer 5.5 и по-нов, Mozilla Firefox 2.0 и по-нов, Сафари

поддръжка	
Single Sign-On	Поддръжка на единично влизане
Протоколи за маршрутизация	Поддръжка на минимум следните маршрутизиращи протоколи: BGP, OSPF, RIPv1 и RIPv2
Мултикаст протоколи	Поддръжка на минимум следните мултикаст протоколи PIM-DM/SM/SSM, IGMP, DVMRP
Система за откриване и предотвратяване на прониквания	Устройствата трябва да имат допълнителна функционалност за откриване и предотвратяване на прониквания. Да се включат всички необходили лицензи и софтуерни обновявания на сигнатурите за 3 години, ако са приложими.
IPS	IPS система трябва да осигури поддръжка за: • Vulnerability and exploit signatures • Protocol validation • Anomaly detection • Behavior-based detection • Multi-element correlation
Сигнатури	Да поддържа създаването на собствени сигнатури с отворен език за писане на сигнатури
IPS профили	Устройството трябва да има дефинирани фабрично профили за максимална защита или за оптимизирана производителност
Улавяне на пакети	Устройството трябва да има функционалност да изследва трафика подробно на ниво пакети
DoS Атаки	Разширена защита срещу атаки "отказ на услуга" (Denial of Service)
Гео защити	Устройството трябва да позволява или да ограничава достъпа на базата на географското местоположение на трафика
Проверка на SSL криптиран трафик	Устройството трябва да сканира и защити SSL криптиран трафик преминаващ през шлюза
Application detection and usage control	Устройството трябва да осигури модул за защита в състояние да идентифицира, да позволи трафик, да блокира или ограничи потреблението (въз основа на честотната лента и/или време) на повече от 240,000 приложения, включително Web 2.0 и социалните мрежи, независимо от порт, протокол или заобикаляща техники да преминат през мрежата.
Динамична URL поддръжка	Устройството да има и динамично да актуализира база данни от над 100 милиона сайта, за да позволява, блокира или ограничава достъпа до уеб сайт в реално време на целия трафик. Да има избор от поне 60 предварително определени съдържателни категории.
URL контрол	Устройството да позволява, блокира или ограничава достъпа до уеб сайт, базиран на потребител, група и дори машинно ID за един URL или цяла категория URL.
Anti-Spam	Устройството трябва да има функционалност за филтриране на нежелани спам съобщения чрез блокиране или маркиране
IP Репутационен Anti-Spam	Устройството трябва да блокира спам и зловреден софтуер на ниво връзки, чрез проверка на репутацията на изпращача от динамична база данни от известни злонамерени адреси
Съдържателно-базиран Anti-Spam	Трябва да защитава срещу напредналите форми на спам, включително изображения и спам на чужди езици, използвайки модел базирано откриване
Anti-Spam функции	Устройството трябва да блокира или разрешава списъци, които се използват за да се премахнат очевидни нарушители

	на електронна поща и да позволи надеждни податели
Zero-hour Outbreak Protection	Устройството трябва да осигури, защитен механизъм срещу атака на нов тип спам и зловреден софтуер чрез Zero-hour Outbreak Protection
Mail Antivirus	Устройството трябва да защитава срещу широк спектър от вируси и зловреден софтуер и да включва сканиране на съдържанието на съобщението и прикачените файлове
Мрежови интерфейси	Устройството да разполага с минимум 8 x 10/100/1000 T - RJ-45 порта
Оперативна памет	Минимум 4GB
Твърд диск	Минимум 250GB
Пропускателна способност на защитната стена	Минимум 3 Gbps
Пропускателна способност при VPN	Минимум 400Mbps
Пропускателна способност при IPS	Минимум 2 Gbps
Сесии за секунда	Минимум 20 000
Едновременни сесии	Минимум 1 милион
Размер	Максимум 1U
Софтуер за управление и наблюдение	Да притежава софтуер за управление и наблюдение на двете устройства в клъстера

Изпълнителят следва задължително да осигури:

1. Хардуерна поддръжка за 3 години.

2. Всички необходими лицензии за софтуерни приложения и софтуерни обновявания на сигнатурите за 3 години, ако са приложими.

3. Инсталиране и конфигуриране на устройствата за мрежова и информационна защита.

4. Поддръжка и обслужване на устройствата за своя сметка, включващо всички разходи - транспорт, труд, резервни части и материали и др., включително замяна на повреденото изделие с оборотно за времето на ремонта с параметри, не по-лоши от дефектиралите;

5. Обслужването и поддръжката с време на реакция до 2 часа след писмено уведомление, включително и по факс или електронна поща в рамките на работното време от 9.00 до 17.30 часа, а ако заявката е постъпила след края на работното време, до 10.00 часа на следващия работен ден.

6. Срокът за отстраняване на повредата е до 4 часа, ако уведомлението е постъпило, в рамките на работното време от 9.00 до 17.30 часа и до 13 часа на следващия работен ден, ако заявката е постъпила след края на работното време;

7. Обучение на трима служители от дирекция „ИКО” за работа с устройствата за мрежова и информационна защита.

Двата броя устройства за мрежова и информационна защита да са идентични, нови, оригинални и неупотребявани.

Доставката следва да се извърши в срок от 40 работни дни след подписването на договора.