Приложение № 2
към рамков договор № № ПО 16-3109/11.10.2024 г.

ЗАЯВКА по Рамков договор № № ПО 16-3109 от 11.10.2024 г.	☑
ЗАЯВКА по Рамков договор № ПО 16-3109 от 11.10.2024 г. (актуализирана)	☐ [1]

Позиция от ПГ-2025 г.:	*№ по ред от ПГ*	*7*
Описание на проект съгласно ПГ:	*Доставка на хардуерни и софтуерни ресурси* *Дейност 1 – Доставка на хардуерни и софтуерни ресурси за 2025 г.*	
CPV код	*48600000-4*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*МЕУ-12293/22.08.2025г.*	
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*	*408,333,00 лв.*
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*На части, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на всяка извършена доставка/услуга по съответната дейност и издадена фактура.*
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 15.12.2025 г.*
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)*	*На части, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на всяка извършена доставка/услуга по съответната дейност и издадена фактура.*
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	

[1] Отбелязва се в случай че заявката е актуализирана

ВЪЗЛОЖИТЕЛЯ:	
Ръководител на договора от страна на БЕНЕФИЦИЕРА:	
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:	
Ръководител на проект по заявката	
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД	

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

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА

ДОСТАВКА НА ХАРДУЕРНИ И СОФТУЕРНИ РЕСУРСИ

ЗА

СМЕТНА ПАЛАТА НА РЕПУБЛИКА БЪЛГАРИЯ

1. ЦЕЛ

Целта на заявката е да се осигурят хардуерни и софтуерни ресурси за нуждите на Сметна палата на Република България.

2. ОБХВАТ

В обхвата на заявката са включени следните дейности:

2.1. Доставка на сървър със следните технически характеристики:

Минимални технически изисквания:		
REQ.1.	Количество	1 броя сървъри за монтаж в 19‘‘шкаф
REQ.2.	Процесор	Минимум 2 Intel® Xeon® Scalable, минимум 16 ядра на процесор, минимум 2.5GHz, минимум 38MB Cache
REQ.3.	Памет	• Поддръжка на 16 DDR5 DIMM slots, поддържани памети RDIMM • Разширяемост до минимум 1TB • Системата да бъде доставена с 8 x 64GB / 4800MT/s
REQ.4.	Устройства за зареждане на операционна система	Системата трябва да бъде доставена с 2 x 480GB SSD Drives, конфигурирани в RAID 1
REQ.5.	Свързаност	Системата да бъде доставена с минимум: - 2 x 10/25 GB SFP+ и 2 x 1Gbit BaseT порта Да бъдат предвидени 2 броя 10Gbase SR SFP+ модула
REQ.6.	Портове и слотове за разширение	• 2 x USB 3.0 & 1 x USB2, VGA • 2 x GEN 5 PCI
REQ.7.	Захранване	Системата трябва да бъде доставена с 2 захранвания конфигурирани в режим 1+1
REQ.8.	Размери	Системата трябва да бъде в размер 1U
REQ.9.	Управление и интеграция	Конзола за управление, която да поддържа интеграция със: Microsoft System Center, VMware vCenter™, Nagios & Nagios XI, IBM Tivoli Netcool/OMNIbus, IBM Tivoli Network Manager
REQ.10.	Система за управление	• Решението трябва да бъде доставено с конзола за управление, която предоставя следните възможности: ○ Virtual Appliance based deployment model and should support ESX,

		Hyper-V, and Citrix o HTML 5 Compliant o Redfish enable REST API support o Firmware/BIOS updates and Compliance o Server configuration profiles and compliance o Bare metal deployment o Fully agent-free management o Must able to scale up to 5000+ server in a single console with no additional licenses o AD integration o Customized reports, and server warranty information. o Mobile integration and call home support o Stateless management, policy-driven event management and notification
REQ.11.	Вградено управление	Системата трябва да бъде доставена с възможности за вградено управление (IPMI compliant, Lifecycle controller, optional wireless). Трябва да поддръжа HTML5 GUI, WS-MAN, Redfish.
REQ.12.	Сигурност	Системата трябва да бъде доставена с TPM 1.2/2.0, cryptographically signed firmware, Secure Boot, System Lockdown, Secure erase security features. Silicon root of trust, Write locking of firmware image during runtime, Automatic BIOS / OS recovery, Dynamically enabled USB ports, system drift detection, TGC UEFI, NIST compliance.
REQ.13.	Поддържани операционни системи	• Canonical® Ubuntu® LTS • Microsoft Windows Server® with Hyper-V • Red Hat® Enterprise Linux • SUSE® Linux Enterprise Server • VMware® ESXi
REQ.14.	Допълнителни възможности	• Must support Connection View provides the switch and port for management module, LOM's and supported PCIe cards. • Must be provided with Virtual Machine Power Mapping capability to facilitate workload balancing and reporting based on power consumption. • Secure at server management capability using a smartphone (IOS / Android) over Ble/WIFI. Able to configure IPMI OOB management IP address, password, NIC configuration, boot order, location and – very importantly – key BIOS attributes. View server inventory, health status, and logs through Bluetooth technology for much

		better “touch & roam.” • Embedded phone home support. Out of Band Call home functionality without any agent or OS interaction.
REQ.15.	Гаранция	36 месеца от вида 8x5xNBD

2.2. Доставка на SAN комутатор със следните технически изисквания:

Минимални технически изисквания	
REQ.1.	Тип на кутията/шасито – 1RU за директен монтаж в 19“ шкаф.
REQ.2.	Да са окомплектовани с резервирано захранване N+1 от 220-240v AC, 50Hz
REQ.3.	Работен температурен диапазон от 0º до +40 ºC.
REQ.4.	Работна относителна влажност от до 85% .
REQ.5.	Минимум 16 SFP порта поддържащи 4/8/16/32 Gbps Fibre Channel, с лицензирани минимум 8 SFP активни порта
REQ.6.	Да има възможност за добавяне на допълнителен модул с 16 SFP порта поддържащи 4/8/16/32 Gbps Fibre Channel.
REQ.7.	Комутатора да бъде доставен с 8 броя 16 Gbit/s FC SFP работещи по мултимод (OM2) влакно на разстояние поне 150 метра.
REQ.8.	Брой USB портове - минимум 1.
REQ.9.	Ethernet порт за управление - минимум 1.
REQ.10.	Сериен конзолен порт - минимум 1.
REQ.11.	Комутатора да поддържа in-band управление чрез IP върху FC.
REQ.12.	Комутатора за поддържа IP ACL на мениджмънт интерфейса си.
REQ.13.	VSAN изолация.
REQ.14.	Хардуерно зониране на база ACL.
REQ.15.	FC-SP автентикация между портовете на два комутатора. FC-SP автентикация между комутатор и хост.
REQ.16.	Комутатора да притежава производителност, позволяваща едновременната работа на всички порта със скорост 32Gbit/s.
REQ.17.	Комутатора да поддържа конфигуриране на QoS. Тежестта на опашките да е конфигурируема.
REQ.18.	Комутатора да поддържа минимум 500 буфер кредита на порт.
REQ.19.	Комутатора да поддържа конфигурирането порт с поне 8000 буфер кредита.
REQ.20.	Комутатора трябва да поддържа премахването на развалени фреймове на база на CRC проверка. Фрейма не трябва да бъде предаван извън комутатора.
REQ.21.	Комутатора да позволява обединяването на поне 16 физически линка в един логически.
REQ.22.	Комутатора да позволява обединяването на портове, които не са поредни.
REQ.23.	Комутатора да поддържа REST API.
REQ.24.	Комутатора да отговаря на следните регулаторни изисквания: • EN55022 Class A • CISPR22 Class A • EN55024

	• EN50082-1 • EN61000-3-2 • EN61000-3-3 • EN61000-6-1 • EN 60950
Гаранция и поддръжка:	
REQ.25.	Срок на хардуерната гаранция - минимум 3 (три) години.
REQ.26.	Срок на техническа поддържка – минимум 3 (три) години.
REQ.27.	Получаване на нови версии на софтуера - минимум 3 (три) години.

2.3. Осигуряване на хардуерна и софтуерна поддръжка за текущ дисков масив Lenovo

2.3.1. Осигуряване на хардуерна поддръжка със следните технически изисквания:

Техническа изисквания:	
REQ.1.	Подновяване на поддръжка на дисков масив Lenovo ThinkSystem DE4000H Hybrid Flash Array SFF със сериен номер S4CLM055
REQ.2.	Получаване на актуални версии на фърмуер
REQ.3.	Поддръжката да е от тип NBD 11x5
Поддръжка:	
REQ.4.	Срок на поддръжка и възможност за обновяване: 12 месеца

2.3.2. Осигуряване на лицензи и софтуерна поддръжка със следните технически изисквания:

Техническа спецификация	
REQ.1.	Име на продукта: Microsoft SQL Server Std Core 2 LSA
REQ.2.	Количество - брой лицензи: 4
REQ.3.	Да бъде осигурена последната налична версия, спрямо актуалната в датата на подаване на офертата
Поддръжка:	
REQ.4.	Срок на поддръжка и възможност за обновяване: 36 месеца

Техническа спецификация	
REQ.1.	Име на продукта: Windows Server Std 2 Core
REQ.2.	Количество - брой лицензи: 104

REQ.3.	Да бъде осигурена последната налична версия, спрямо актуалната в датата на подаване на офертата
Поддръжка:	
REQ.4.	Срок на поддръжка и възможност за обновяване: 36 месеца

Техническа спецификация	
REQ.1.	Име на продукта: Exchng Svr Ent Svr LSA
REQ.2.	Количество - брой лицензи: 2
REQ.3.	Да бъдат осигурени Exchng Svr Std User CALSA за 450 потребителя
REQ.4.	Да бъде осигурена последната налична версия, спрямо актуалната в датата на подаване на офертата
Поддръжка:	
REQ.5.	Срок на поддръжка и възможност за обновяване: 36 месеца

2.4. Доставка на решение за централизирано автентикиране на потребителите със следните технически характеристики:

Минимални технически изисквания	
REQ.1	Инсталация - виртуална машина с поддръжка на VMWare ESXi, Linux KVM и Microsoft Hyper-V.
REQ.2	Минимум две виртуални машини в режим на резервиране. Отпадането на едната виртуална машина не трябва да влияе на работоспособността на услугите.
REQ.3	AAA услуги за потребители и устройства.
REQ.4	Вградени WEB/Captive портали за идентификация на потребителите.
REQ.5	API интерфейс за интеграция с външни системи за отчетност и мрежови политики.
REQ.6	Интеграция с външни сървъри за идентификация - Microsoft Active Directory, LDAP, RADIUS, RSA системи за идентификация с еднократна парола.
REQ.7	Удостоверяване чрез потребителско име и парола, с X.509 сертификат и по MAC адрес.
REQ.8	Профилиране на крайните устройства.
REQ.9	BYOD функции.
REQ.10	Прилагане на различни политики за удостоверяване и оторизация на база: • Час и дата на идентификацията • Тип на връзката – 802.1x wired, 802.1x wireless, достъп през VPN , достъп през WEB портал за идентификация • Използван EAP тип • Потребителско име

	• RADIUS атрибути • Атрибути на X509 потребителските сертификати • Вид/модел/OS на устройството
REQ.11	Управление на мрежовия достъп: • Динамично зареждане на филтриращи листи (ACL) в мрежовите устройства на база политиките за управление на достъпа. • Динамично назначаване на VLAN мрежи към потребителите на база политиките за управление на достъпа. • URL пренасочвания на потребителите към вградени или външни WEB/Captive портали.
REQ.12	Поддръжка на RADIUS и Radius CoA.
REQ.13	Възможност за добавяне на TACACS+ за идентификация и управление нивото на достъп на администраторите към мрежови устройства.
REQ.14	Възможност за добавяне на функционалност за проверка на състоянието (posture assessment) на крайните потребители.
REQ.15	Функция на RADIUS proxy.
REQ.16	Вграден Certificate Authority.
REQ.17	• Web GUI • HTTP и HTTPS • Ping • DNS • TFTP • FTP • NTP • SSHv2 • Интеграция с LDAP • Автоматичен backup на базата данни върху външни FTP и SFTP сървъри
REQ.18	• Да бъдат предложени лицензи за удостоверяване и оторизация на 350 крайни устройства едновременно.
REQ.19	• Да бъдат предложени лицензи осигуряващи непрекъсваемост на услугите предвидени в REQ.2.
Гаранция и поддръжка	
REQ.20	Техническа поддръжка за срок от 3 (три) години.
REQ.21	Получаване на нови версии на софтуера за срок от 3 (три) години.
REQ.22	Лицензни абонаменти за използване на софтуерни функции за срок от 3 (три) години.

2.5. Доставка на система за защита и инспекция на DNS трафика със следните технически характеристики:

Минимални технически изисквания	
REQ 1	DDI Системата (DNS, DHCP & IP Address Management) трябва да бъде доставена като готов за използване OVA образ с възможност за интегриране във VMware среда, която Възложителят вече притежава.
REQ 2	Системата трябва да предоставя услуга за управление на IP адреси – IPAM (IP Address Management)
REQ 3	Системата трябва да разполага с механизми за контрол на въвежданите данни (коректност на IP адреси, маски и др.)
REQ 4	Системата трябва да позволява добавяне на описания и атрибути за мрежови обекти, IP адреси, домейни. Тези атрибути трябва да имат възможност за дефиниране на типа и размера им
REQ 5	Системата трябва да поддържа механизъм за сканиране на мрежи и хостове/IP адреси (т.нар. network discovery)
REQ 6	Системата трябва да поддържа функции като „намери 10 неизползвани адреса от мрежа X“ и „намери 10 неизползвани подмрежи с размер напр. /24 в подмрежа напр. abcd/16“. Функцията трябва да бъде налична за IPv4 и IPv6
REQ 7	Системата трябва да позволява импортиране на данни в CSV формат директно от графичния интерфейс и да разполага с подробна документация за формата на импортираните данни
REQ 8	Капацитетът на DNS/DHCP/IP базата данни трябва да бъде за минимум 100000 записа.
REQ 9	Системата трябва да позволява интеграция с VMware vCenter и OpenStack услуги, за да извършва процес на откриване на виртуални машини, работещи във VMware/OpenStack инфраструктура, и автоматично да създава DNS записи за тези машини
REQ 10	Системата трябва да поддържа внедряване на DHCP услуги за IPv4 и IPv6 с минимална производителност от 200 DHCP leases в секунда
REQ 11	Системата трябва да поддържа актуализиране на DDNS данни чрез DHCP услугата
REQ 12	Системата трябва да поддържа актуална информация за разпределените IP адреси и устройствата, на които е присвоен даден адрес (MAC адрес, време и дата на присвояване на адреса, IP)
REQ 13	Системата трябва да поддържа функционалност DHCP Failover с възможност за повторно договаряне на наличните адресни пространства
REQ 14	Трябва да бъде възможно проверката за наличност на IP адрес преди неговото разпределяне чрез ICMP
REQ 15	Системата трябва да разпознава типа на устройството/системата на станции, мобилни устройства и др. въз основа на анализа на DHCP заявката. Трябва да поддържа отчет за типа на устройството в историята на DHCP наемите и да предоставя възможност за филтриране/блокиране на разпределението на адреси за избрани типове устройства (напр. разпределяне на адрес за Windows станция, но не и за таблет или смартфон)
REQ 12	Системата трябва да предоставя авторитетни и рекурсивни услуги за разрешаване на домейн имена (DNS - Domain Name System)
REQ 13	Производителността на авторитетния DNS трябва да бъде поне 10 000 DNS заявки в секунда
REQ 14	Системата трябва да изпълнява автоматични DNS актуализации в съответствие с RFC 2136
REQ 15	Системата трябва да разполага с вграден механизъм за уведомяване при

	промени в зоните, в съответствие с RFC 1996
REQ 16	Системата трябва да поддържа DNS протоколи както за IPv4, така и за IPv6
REQ 17	Системата трябва да поддържа DNS Anycast услуга за IPv4 и IPv6 (използвайки BGP и OSPF протоколи)
REQ 18	Системата трябва да поддържа DNSSEC услуга с автоматично обновяване на подписите при промени в DNS зоните
REQ 19	Системата трябва да поддържа DDNS услуга
REQ 20	Системата трябва да поддържа защитено обновяване на DNS записи с поддръжка на GSS-TSIG протокол
REQ 21	Системата трябва да поддържа MultiMaster DNS функционалност
REQ 22	Системата трябва да поддържа механизъм за IDN (Internationalized Domain Names) и да разполага с вграден конвертор за punycode (поддръжка на кирилица)
REQ 23	Системата трябва да поддържа IDN за DNSKEY записи, DS записи, NSEC записи, NSEC3PARAM записи и RRSIG записи
REQ 24	Системата трябва да поддържа EDNS0 разширения съгласно стандарта RFC 6891
REQ 25	Системата трябва да поддържа следните алгоритми за публични ключове, използвани с DNSSEC: DSA, RSA/MD5, RSA/SHA1, RSA/SHA-256, RSA/SHA-512, ECDSAP/SHA-256, ECDSAP/SHA-384
REQ 26	Подписаните с DNSSEC зони трябва да поддържат динамични DNS актуализации
REQ 27	Системата трябва да поддържа автоматично подписване на DNS записи след промени
REQ 28	Системата трябва да функционира като платформа за разпространение на файлове чрез протоколите TFTP, FTP, HTTP и да предлага услуги за синхронизация на времето чрез NTP (Network Time Protocol)
REQ 29	Системата трябва да работи под контрола на специализирана операционна система. Използването на операционни системи с общо предназначение не е разрешено. Тя не трябва да зависи от или да изисква конкретни версии на операционни системи с общо предназначение или програмни библиотеки
REQ 30	Управлението на системата трябва да се осъществява чрез уеб браузър, без да е необходимо инсталирането на допълнителен софтуер като агент, клиент и др
REQ 31	Възможност за управление от няколко системни администратори, вписани едновременно
REQ 32	Системата трябва да предоставя възможност за управление на IPv4 и IPv6 адреси, позволявайки графичен, конзолен, и API интерфейси
REQ 33	Системата трябва да поддържа удостоверяване на потребители чрез: - Локална потребителска база - RADIUS протокол - TACACS+ протокол - LDAP - Microsoft Active Directory
REQ 34	Системата трябва да има вградена база данни за съхранение на DDI информация. Базата данни не трябва да изисква поддръжка, свързана с нейната конфигурация и управление
REQ 35	Системата трябва да може да бъде наблюдавана чрез SNMP (Simple Network Management Protocol)
REQ 36	Системата трябва да позволява планирани резервни копия (backups) към външен сървър, за да улесни възстановяването в случай на бедствие (чрез TFTP, FTP, SCP)

REQ 37	Системата трябва да поддържа интеграция с инструменти за управление на конфигурацията като Ansible, Puppet и Chef
REQ 38	Системата трябва да поддържа възможност за импортиране и експортиране на данни в различни формати, включително CSV и JSON
REQ 39	Устройството трябва да разполага с функционалност за разпознаване и блокиране на DNS тунелиране чрез аналитичен механизъм, базиран на машинно обучение, който разпознава неизвестни модели на тунелиране и извличане на данни чрез DNS. Системата трябва да анализира поне 10 атрибута на всяка DNS заявка, включително: ентропия на символите във FQDN, популярност на дву- и трибуквени комбинации, съотношение на гласни в FQDN, съотношение на цифри, размер на заявката, честота и промяна на честотата на DNS заявките
REQ 40	В рамките на приемателните тестове, възложителят ще извърши тест за откриване на DNS ексфилтрация. Тестът ще се проведе с персонализиран скрипт, генериращ между 100 и 200 DNS заявки с интервал от 2,5-3,5 секунди
REQ 41	Системата трябва да разполага с функционалност за откриване на проникванията през DNS, по-специално трябва да разпознава техниката, използвана от зловредния софтуер Powersource/DNS Messenger, и да блокира опити за пренос на данни, кодирани в DNS отговори чрез TXT записи
REQ 42	Системата трябва да разполага с функционалност Response Policy Zones (RPZ) за работа като DNS защитна стена въз основа на списъци с опасни домейни
REQ 43	Системата трябва да регистрира и предоставя информация за всички промени, направени от администратори (кой, кога, какво е променил)
REQ 44	Системата трябва да може да изпраща логове към централен хранилищен сървър чрез Syslog механизъм (TCP и UDP)
REQ 45	Системата трябва да позволява администраторите да имат права, базирани на групи и роли, които ограничават достъпа им само до необходимите ресурси. Подробните разрешения трябва да позволяват конфигуриране на права за отделни обекти, като мрежи, DNS зони и конкретни DNS записи.
REQ 46	Системата трябва да поддържа криптирана комуникация между компонентите си чрез TLS (Transport Layer Security)
REQ 47	Достъпът до административния интерфейс трябва да бъде защитен чрез двуфакторна автентикация (2FA)
REQ 48	Системата трябва да предоставя механизъм за защита срещу неоторизиран достъп чрез прилагане на списъци за контрол на достъпа (ACL)
REQ 49	Системата трябва да поддържа защита от атаки тип DDoS срещу DNS и DHCP услуги
REQ 50	Системата трябва да поддържа механизъм за мониторинг и алармиране при откриване на аномалии в мрежовия трафик, свързан с конфигурираните услуги
REQ 51	Системата трябва да има възможност за запис и анализ на потребителските сесии в административния интерфейс за целите на одит и сигурност
REQ 52	Системата трябва да поддържа криптиране на чувствителни данни в конфигурационните файлове и базата данни
REQ 53	Системата трябва да позволява дефиниране на политики за автоматично деактивиране на потребителски акаунти при откриване на подозрителна активност

REQ 54	Услугата трябва да има възможност да предприема действия по DNS заявки и отговори въз основа на дефинирани от клиента правила за защита - Възможните действия трябва да включват: разрешаване на заявка без регистриране, разрешаване на заявка с логиране, блокиране на заявка с NXDomain отговор (няма такъв домейн), пренасочване (отговор с дефиниран IP адрес). Пренасочването трябва да е възможно към уеб страница, предоставена от доставчика. Системата трябва също така да позволява пренасочване към всеки IP адрес. - Системата трябва да предприеме действия въз основа на името на домейна в заявката и въз основа на IP адреса в отговора. Действието върху името на домейн трябва да работи за всеки тип заявка – системата не трябва да позволява заобикаляне на блокирането чрез изпращане на специфични типове заявки като SOA или NS. Системата не трябва да позволява заобикаляне на блокирането на злонамерен домейн чрез изпращане на запитвания с главни или смесени FQDN (DNS протоколът е нечувствителен към малки и големи букви, а сигурната DNS система също трябва да е нечувствителна към малки и големи букв - Системата трябва да позволява да се дефинира персонализиран списък с домейни/IP адреси, по които да се действа, и също така трябва да предоставя списък с домейни и IP адреси под формата на емисии за заплахи, дефинирани по-долу. За персонализирани списъци системата трябва да има възможност да дефинира нивото на заплаха и увереността на заплахата за всеки списък. Системата трябва да позволява създаване и редактиране на персонализирани списъци от клиентския портал, както и чрез API, за да позволи лесно импортиране на персонализирани данни за заплахи. - Системата трябва да предоставя възможност за заобикаляне на блокове със специфични кодове, предоставени на избрани потребители
REQ 55	Трябва да е възможно изпращането на DNS заявки към услуга предоставяща функции за категоризирането и филтрирането им - от персонализирано дефинирана IP мрежа - от DMZ DNS сървъри, сървърите трябва да добавят вътрешен IP адрес на клиента вътре в заявките и да ги изпращат в криптирана форма към услугата - От роуминг агент, предоставен от доставчика. Роуминг агентът трябва да бъде предоставен за Windows, Mac OS, Android и iOS Данните за заплахите, предоставени от доставчика, трябва да включват - списък на интернет домейни, свързани с APT атаки - списък с домейни и IP адреси, свързани със злонамерен софтуер - Списък с домейни, свързани с рансъмуер - списък с IP адреси, свързани с ботнет мрежи - списък на домейните, свързани със злонамерен софтуер, с помощта на алгоритми за генериране на домейни (DGA) - списък с IP адреси на изходните възли на TOR мрежата - списък с домейни, свързани с фишинг - списък на домейните, свързани с неоторизирано копаене на криптовалута - списък на домейните, регистрирани през последните три дни. Данните за новите регистрации трябва да идват от най-малко 500 различни домейна от първо ниво (домейни от първо ниво). - Списък на домейни, които споделят подозрителни характеристики като примерни домейни, са регистрирани по едно и също време от същия регистрант, който в миналото е регистрирал домейни, за които е доказано, че са свързани със злонамерена дейност
REQ 56	Всички горепосочени списъци за заплахи трябва да бъдат налични за конфигуриране в политиката за защитени DNS услуги, както и във формат

	RPZ, за да бъдат изтеглени на DNS сървъритею
REQ 57	Списъците за заплахи от доставчика трябва да бъдат достъпни чрез API във формати CSV, STIX, XML, JSON и CEF за използване в други системи за сигурност като SIEM, защитни стени или защитени уеб шлюзове
REQ 58	Разузнаването на заплахите трябва да може да предоставя контекстуална информация за домейн/IP, поне трябва да включва данни, ако заплахата е свързана с ексфилтрация на данни, влияе ли върху наличността на системите, необходимо ли е взаимодействие с потребителя за активиране на заплахата, какви техники са включени
REQ 59	Защитената DNS услуга трябва да има функционалността за откриване и блокиране на DNS тунелиране с помощта на аналитичен алгоритъм, базиран на машинно обучение и позволяващ откриване на неизвестни модели на тунелиране и ексфилтрация на данни през DNS. Системата трябва да анализира поне 10 атрибута на всяка DNS заявка и това трябва да включва: ентропия на знаците в FQDN, оценяване на всеки набор от 2 и 3 знака за популярност в естествените езици, изчисляване на съотношението на гласните в FQDN, изчисляване на съотношението на цифрите в FQDN, анализиране на размера на заявката, анализиране на честотата на DNS заявките (стойност на честотата и промяна на честотата). Защитената DNS услуга трябва да открива DNS тунелиране, независимо от категорията на съдържанието на домейна, използван в DNS заявката
REQ 60	Защитената DNS услуга трябва да има функционалност за откриване на непознати DGA и DGA домейни в DNS заявки
REQ 61	Защитената DNS услуга трябва да има информация за категорията съдържание за домейни и трябва да може да действа по нея, например трябва да предоставя възможност за предприемане на действия за домейни, хостващи съдържание като порно, опасност, социални мрежи, анонимайзери и др.
REQ 62	Системата трябва да поддържа механизми за висока наличност (High Availability - HA) за всички основни услуги, включително DNS, DHCP и IPAM
REQ 63	Системата трябва да поддържа клъстеризация на компонентите си с цел осигуряване на надеждност и отказоустойчивост
REQ 64	Системата трябва да позволява автоматично превключване (failover) при отпадане на даден сървър или услуга
REQ 65	Системата трябва да поддържа географски разпределено внедряване с възможност за репликация на данни между различни локации
REQ 66	Системата трябва да има механизъм за автоматично балансиране на натоварването (load balancing) между DNS и DHCP сървърите
REQ 67	Системата трябва да осигурява непрекъсната работа при актуализации (Rolling Updates), без да се нарушава функционирането на критичните услуги
REQ 68	Системата трябва да позволява възстановяване след срив (Disaster Recovery) чрез механизъм за архивиране и репликация на данни
REQ 69	Системата трябва да поддържа синхронизация на конфигурацията и данните между главните и резервните инстанции в реално време
REQ 70	Бързо възстановяване на услугите в случай на срив, като времето за възстановяване не трябва да надвишава 10 минути.
REQ 71	Системата трябва да предоставя централизирана отчетност за всички DNS, DHCP и IPAM събития

REQ 72	Системата трябва да поддържа механизъм за събиране и анализ на логове, включително възможност за интеграция с SIEM (Security Information and Event Management) решения
REQ 73	Системата трябва да позволява генериране на персонализирани отчети за използването на IP адреси, DHCP лизинги и DNS заявки
REQ 74	Системата трябва да осигурява механизъм за известяване на администраторите чрез имейл, SNMP трап (trap) или уеб интерфейс при откриване на критични събития
REQ 75	Системата трябва да предоставя детайлни статистики за производителността на DNS и DHCP услугите, включително натоварване, време за отговор и брой заявки
REQ 76	Системата трябва да позволява интеграция със системи за мрежов мониторинг чрез SNMP (v2c и v3)
REQ 77	Системата трябва да предоставя исторически данни за заетостта на IP адресите и тенденциите на използване
REQ 78	Системата трябва да поддържа механизъм за автоматично архивиране на логове и отчети за последващ анализ
REQ 79	Системата трябва да позволява конфигуриране на политики за съхранение и изтриване на исторически данни
REQ 80	Системата трябва да може да визуализира информацията чрез графики и диаграми в уеб интерфейса
REQ 81	Порталът за защитени DNS услуги трябва да предоставя възможности за отчитане. Докладите трябва да включват: - Отчети за дейността, показващи DNS заявки, изпратени до услугата - Отчети за защитата, показващи DNS заявки, които засягат правилата за сигурност - Трябва да има възможност за изпращане на изходни данни (заявки, събития за защита) до локална SIEM система под формата на съобщения в системен дневник или директна интеграция
REQ 82	Достъпът до клиентския портал трябва да се основава на потребителски данни за вход със специфични роли за достъп, като например достъп само за четене или административен достъп. Промените в конфигурацията на DNS услугата трябва да бъдат регистрирани в регистрационния файл за проверка.
REQ 83	Висока производителност с минимално време за отговор на DNS заявки (не по-високо от 50 милисекунди) при натоварване до 5 хиляди заявки на секунда.
REQ 84	Поддържка на DHCP услуги с производителност минимум 200 заявки на секунда.
REQ 85	Надеждност при обработка на големи обеми данни и да не претоварва мрежовата инфраструктура при високи натоварвания.
REQ 86	Възможност за работа с разширени DNS записи и поддържа функционалности като DNSSEC и Anycast без да се нарушава производителността.
REQ 87	Възможност за обработка на натоварвания, които включват обработка на над 30 милиона DNS заявки и DHCP лизинги месечно.
REQ 88	Възможност за динамично регулиране на ресурсите според натоварването, включително за работа в облачни среди и виртуализирани инфраструктури.
REQ 89	Възможност за интелигентно управление на натоварването и оптимизация на ресурсите чрез използване на технологии като load balancing и autoscaling.
REQ 90	Да бъде в състояние да обслужва нуждите на организацията при неограничено нарастващ обем от мрежови услуги и данни, като остава стабилна и ефективна.

Поддръжка и лицензи	
REQ 91	Системата трябва да е лицензирана за поне 350 потребителя.
REQ 92	DDI Системата трябва да е оразмерена и лицензиране за безпроблемна работа на поне 450 IP адреса.
REQ 93	Поддръжка от производителя, включително получаване на нови версии на софтуера и 24/7 техническа помощ чрез телефон, имейл и портал за заявки за срок от минимум 3 (три) години.
REQ 94	Механизъм за известяване на администраторите за наличието на нови актуализации и критични поправки.

3. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

3.1. Изисквания към изпълнението за точки 2.1, 2.2 и 2.3.1 са следните:

- Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или официален негов представител за право на разпространение на предлаганите продукти на територията на Република България;
- Оборудването трябва да съответства или да надвишава в техническо отношение посочените минимални изисквания в настоящите Технически параметри;
- Оборудването, предмет на доставката, трябва да бъде фабрично ново, неупотребявано, да е в актуалните продуктови листи на производителя и да не е спряно от производство;
- Хардуерните компоненти на оборудването следва да отговарят на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа;
- Хардуерът следва да бъде доставен в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, където се изискват, както и с необходимата техническа документация (на електронен носител или чрез линкове, от които може да бъде свалена);
- В рамките на срока на гаранционно обслужване Изпълнителят отстранява за своя сметка всички повреди и/или несъответствия на оборудването, съответно подменя дефектирали части, устройства, модули и/или компоненти с нови съгласно предписанията на производителя. В гаранционното обслужване се включва замяна на част (компонент) със скрити недостатъци с нова или на цялото устройство с ново, ако недостатъкът го прави негодно за използване по предназначението му, както и всички разходи по замяната;
- Заявки за обслужване (тикети) за доставения хардуер се подават чрез осигурена от Изпълнителя онлайн система за управление на заявки (СУЗ). Всички заявки, получени чрез електронна поща или телефон следва да бъдат регистрирани в СУЗ;
- Режимът на гаранционното обслужване на хардуера е 5 дни в седмицата (от понеделник до петък), 8 часа в рамките на работното време от 9.00 ч. до 17.30 ч. Времето за реакция е до следващия работен ден от уведомяването;
  Време за реакция е времето от момента на уведомяване от страна на Бенефициера за възникнал проблем до обратна реакция (обаждане или пристигане на място) от ангажирани с изпълнението лица;

- Ангажираните с изпълнението лица са длъжни да осигурят преглед на място в срок не по-късно от следващия работен ден от 9.00 ч. до 17.30 ч.;
- Лицето, ангажирано с изпълнението, следва да отстрани настъпилата повреда и/или несъответствие и възстановяване на пълната работоспособност на оборудването. Отстраняването на настъпила повреда и/или несъответствието се осъществява по местонахождението на оборудването;
- За всяка извършена дейност, свързана с гаранционното обслужване, се изготвя и предоставя протокол за извършена дейност по гаранционно обслужване, който съдържа описание на извършеното, включително вид и количество. Протоколът се подписва от ангажирано от Изпълнителя лице и оторизираното лице по място на инсталация;
- При невъзможност за отстраняване на настъпила повреда и/или несъответствие, следва да бъде осигурено оборотно оборудване, притежаващо характеристиките на доставеното устройство, включително нови алтернативни решения при запазване на пълната изисквана функционалност, до пълното отстраняване на повреда или несъответствие, като срока на гаранционно обслужване на оборудването в процес на поправяне, се удължава със срока, през който е траело отстраняването на повредата;
- В случай, че повредата и/ или несъответствието прави устройството негодно за използване по предназначението му, ангажираното с изпълнението лице е длъжно да го замени с ново, с параметри, гарантиращи същата или по-добра функционалност и производителност.

3.2. Изискването към изпълнението на точки 2.3.2, 2.4 и 2.5:

Изпълнителят следва да осигури продуктите от лице, надлежно оторизирано от производителя или негов официален представител за предоставяне на право на ползване и поддръжка на предлаганите софтуерни продукти на територията на Република България.

4. СРОК НА ИЗПЪЛНЕНИЕ:

Срокът на изпълнение е до 15.12.2025 г.

5. МЯСТО НА ИЗПЪЛНЕНИЕ

Мястото на изпълнение е сградата на Сметна палата на Република България, намираща се на адрес: гр. София, ул. „Екзарх Йосиф“ № 37.