Приложение № 3

МИНИСТЕРСТВО НА ТРАНСПОРТА,
ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ И СЪОБЩЕНИЯТА
**ИЗПЪЛНИТЕЛНА АГЕНЦИЯ**
**„ЕЛЕКТРОННИ СЪОБЩИТЕЛНИ МРЕЖИ И ИНФОРМАЦИОННИ СИСТЕМИ"**

**ул. "Ген. Гурко" № 6, София 1000**
**тел.: (+359 2) 949 2115**
**факс: (+359 2) 981 8787**

mail@esmis.government.bg
www.esmis.government.bg

# ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

## КЪМ ОБЯВА ЗА ОБЩЕСТВЕНА ПОРЪЧКА НА СТОЙНОСТ ПО ЧЛ. 20, АЛ. 3 ОТ ЗОП

## С ПРЕДМЕТ:

## „Предоставяне на услуги, свързани с кибернетична защита на мрежовите и информационни ресурси на ИА ЕСМИС"

**2016 г.**

**СЪДЪРЖАНИЕ**

## I. ЦЕЛ НА ПОРЪЧКАТА

Целта на обществената поръчка е осигуряването на кибернетична защита на мрежовите и информационни ресурси на ИА ЕСМИС.

## II. КОЛИЧЕСТВО И МЯСТО НА ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

Поръчката обхваща предоставяне на услуги за кибернетична защита на мрежовите и информационни ресурси на ИА ЕСМИС. Мястото за изпълнение на поръчката е сградата на ИА ЕСМИС, находяща се в гр. София, ул. „Ген. Й. В. Гурко“ № 6.

## III. ОБЩИ И СПЕЦИФИЧНИ ИЗИСКВАНИЯ

1. Услугите, предоставяни от ИЗПЪЛНИТЕЛЯ на ВЪЗЛОЖИТЕЛЯ представляват услуги, платими на месечен абонаментен принцип за срока на действие на договора по Поддръжка и управление на системи и мрежови архитектури свързани с информационната сигурност, както следва:

1.1. Оптимизация и конфигурация на съществуваща мрежова архитектура за нуждите на сигурното и качествено предоставяне на ИТ базирани услуги от ВЪЗЛОЖИТЕЛЯ:

1.1.1. Извършване на анализ на съществуващата мрежова архитектура, както и на структурата и начина на предоставяне на ИТ базирани услуги в мрежата на Възложителя.

1.1.2. Изработване на предложение за оптимизация във връзка с резултатите от анализа. Оптимизация и документиране на извършените дейности в съответствие с възможните сценарии за изпълнението им и изискването за спазване на добрите практики и гарантиране на сигурността на комуникационната инфраструктура и услугите.

1.1.3. Текущ мониторинг на конфигурациите и преконфигуране в съответствие с добрите практики и гарантиране на сигурността на комуникационната инфраструктура и услугите.

1.2. Изготвяне на документация и отразяване на промени на мрежовата архитектура след направените по т. 1.1. дейности.

1.3. Текущ преглед и промени на мрежовата инфраструктура в съответствие с добрите практики и наличните темплейти за конфигурация, дефинирани политики за сигурност, във връзка със защитата и безопасното използване на мрежата на ВЪЗЛОЖИТЕЛЯ.

1.4. Конфигуриране на централизирана система за управление/съхранение на потребителските профили и данни на база функционалности, налични в MS Windows Server 2012.

1.5. Създаване на централизирано хранилище за профили на използваните от Възложителя операционни системи, драйвери и софтуер и създаване на политики за централизирано и автоматизирано управление на процесите по инсталация и преинсталация на крайните потребителски станции на база функционалности, налични в MS Windows Server 2012.

1.6. Предоставяне на консултантски услуги за срока на действие на договора изпълнението на проекти свързани с използване на информационно-комуникационната инфраструктурата на ВЪЗЛОЖИТЕЛЯ, с цел гарантиране на информационната сигурност и спазване на добрите практики при експлоатацията.

1.7. Поддръжка и текущи конфигурации на съществуваща резервирана open source базирана система за балансиране на натоварването в трафика към предоставяните публични услуги на ВЪЗЛОЖИТЕЛЯ.

Системата е изградена на базата на open source имплементация на проекта Zen Load Balancer.

1.8. Поддръжка и текущо конфигуриране на съществуваща резервирана Linux система за управление на външни DNS услуги на ВЪЗЛОЖИТЕЛЯ, изградена върху Debian операционна система.
1.9. Предоставяне на управлявана услуга за активно управление на системи и решения за информационната сигурност:
1.9.1. Управление на конфигурации на системи за информационна сигурност:
2 бр. PALO ALTO NETWORKS PA-3020, инсталирани в резервирана (High Availability) двойка със следните лицензи:

PA-3020 Threat Prevention Subscription for devices in HA pair
PA-3020 PANDB URL Filtering Subscription for devices in HA pair
PA-3020 WildFire Subscription for devices in HA pair
PA-3020 GlobalProtect Subscription for devices in HA pair

McAfee ePolicy Orchestrator Management Server със следните лицензи:
McAfee Complete EndPoint Protection – Business LICENSE

1.9.2. Управление на обновяването на новите версии на операционните системи и софтуера на системи за информационна сигурност.
1.9.3. Проактивно наблюдение и управление на инцидентите свързани с информационната сигурност и реакция в съответствие с разработения План за реакция при инциденти.
1.9.4. Създаване и внедряване на модел на конфигурация на PA-3020 защитна стена, организиран като отделни политики за всяка зона с експлицитен модел на отказ (позитивен модел за сигурност) и добавен контекст чрез спецификация и контекстуално описание на всички услуги, които имат право да съществуват и функционират в съответната зона.
1.9.5. Използване на модела по т. 1.9.4 за сегментиране на управлението на защитната стена и осигуряване на достъп за определени администратори на Възложителя, които да имат право да добавят обекти към вече съществуващите политики на защитната стена. Цел - да се сведат до минимум възможностите за компромитиране, поради потребителски грешки, на глобалната архитектура на защитната стена и дефинираните по зони политики.
1.10. Поддръжка в актуално състояние и обновяване на План за реакция при инциденти. Сроковете за реакция при инциденти, определени с Плана за реакция при инциденти следва да бъдат приведени в съответствие предложените срокове за реакция по т. 1.9 от настоящата Техническа спецификация.
1.11. Поддръжка и обновяване на системата за проактивно, централизирано наблюдение, корелация на събития генерирани от отделните системи за сигурност и мрежовата архитектура, и управление на инцидентите.
1.12. Изготвяне на ежемесечен доклад до 5-то число на месеца следващ месеца на предоставяне на услугите, включващ:
1.12.1 Анализ, препоръки и консултации в съответствие с добрите практики за превенция на заплахите /нови и съществуващи/, идентифицирани посредством описаните в т.1.9.1. Системи за информационна сигурност и съответните техни компоненти.
1.12.2 Подробно описание на инсталираните ъпдейти и ъпгрейди на системите по т. 1.9.2. в едно с направените промени по конфигурациите.
1.13. Споделяне на опит, последващ анализ на инциденти и обучение
1.13.1 Разбор и преглед на дейности във връзка с регистрирани инциденти, описани в документите по т.1.11.1.
1.13.2 Организиране на обучение по теми предложени от Възложителя – 4 пъти за срока на договора на територията на ИА ЕСМИС или дистанционно.

## IV. СРОК И УСЛОВИЯ ЗА ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

**1.** Срокът за изпълнение на обществената поръчка е **1 (една) година**, считано от датата на подписване на договора, удостоверена с регистрационен щемпел на възложителя.
**2.** Възложителят и Изпълнителят определят лица за контакти, които координират качественото и своевременно изпълнение на договора.

## V. ТЕХНИЧЕСКИ ИЗИСКВАНИЯ

Системи и компоненти в обхвата на услугата:

1. Системи за информационна сигурност и техните компоненти, които ще се поддържат и управляват от ИЗПЪЛНИТЕЛЯ:

1.1. 2 бр. PALO ALTO NETWORKS PA-3020, инсталирани в резервирана (High Availability) двойка със следните лицензи:

1.1.1. PA-3020 Threat Prevention Subscription for devices in HA pair
1.1.2. PA-3020 PANDB URL Filtering Subscription for devices in HA pair
1.1.3. PA-3020 WildFire Subscription for devices in HA pair
1.1.4. PA-3020 GlobalProtect Subscription for devices in HA pair

1.2. McAfee ePolicy Orchestrator Management Server със следните лицензи:

McAfee Complete EndPoint Protection – Business LICENSE

2. Инфраструктурни системи и техните компоненти, които ще се поддържат и управляват от ИЗПЪЛНИТЕЛЯ:

2.1. 2 бр. Debian базирани DNS сървъра, инсталирани в резервирана (High Availability) двойка.

2 бр. системи, базирани на Zen Load Balancer open source технология, за балансиране на натоварването в трафика към предоставяните публични услуги, инсталирани в резервирана (High Availability) двойка.