ЗАСТУПНИК ГОЛОВИ
КОМІТЕТУ З КОНКУРСНИХ ТОРГІВ

_____ Бартащук О. І.

21» серпня 2015 р.

Протокол засідання ККТ від 21.08.2015 № 7

ЗАПИТ
цінових пропозицій

1. Замовник.
1.1. Найменування: ***Фонд державного майна України.***
1.2. Код за ЄДРПОУ: ***00032945***
1.3. Місцезнаходження: ***вул. Кутузова, 18/9, м. Київ-133, 01601***
1.4. Реєстраційний рахунок замовника: ***35216001005357***
1.5. Посадові особи замовника, уповноважені здійснювати зв'язок з учасниками (прізвище, ім'я, по батькові, посада та адреса, номер телефону та телефаксу із зазначенням коду міжміського телефонного зв'язку, електронна адреса): - ***Воронін Микола Володимирович – начальник відділу інформаційного забезпечення, тел. (044) 200-31-68, Леонова Юлія Михайлівна – головний спеціаліст відділу по роботі з питань державних закупівель, тел. (044) 200-33-40, вул. Кутузова, 18/9, м. Київ-133, 01601.***
2. Розмір бюджетного призначення за кошторисом або очікувана вартість предмета закупівлі***: 190000,00 грн, (сто дев'яносто тисяч грн. 00 коп.)***
3. Адреса веб-сайта, на якому замовником додатково розміщується інформація про закупівлю: ***www.spfu.gov.ua***
4. Інформація про предмет закупівлі.
4.1. Найменування предмета закупівлі: ***послуги щодо видання ліцензії на право користування програмним забезпеченням (код 58.29.5 згідно з ДК 016:2010) (послуги з постачання антивірусного ліцензійного програмного забезпечення).***
4.2. Опис предмета закупівлі чи його частин (якщо замовник передбачає подання цінових пропозицій за частинами), у тому числі їх необхідні технічні та інші параметри:

За умовами запиту повинні бути надані послуги з постачання антивірусного програмного забезпечення (ліцензія для 635 робочих станцій та 65 серверів), яке буде використовуватися в корпоративній мережі державних органів приватизації.

Строк дії ліцензії – 1 рік.

З ліцензією повинні бути поставлені електронний носій інформації з примірником програмного забезпечення та експлуатаційна документація. Експлуатаційна документація може бути поставлена на електронному носію інформації.

Технічна підтримка та гарантійне обслуговування програмного забезпечення з боку постачальника ПЗ протягом строку дії ліцензій повинно включати в себе:
- оновлення антивірусних баз та програмного забезпечення;
- підтримка постійно діючої гарячої телефонної консультативної лінії, що працює в робочі дні з 9-30 до 18-00;
- інформування фахівців Замовника про попереджувальні заходи та надання методичної та технічної допомоги у разі виникнення поширених загроз атак засобами електронної пошти при підписці на сайті виробника.

Антивірусне програмне забезпечення має бути сертифіковане уповноваженим органом та мати чинний експертний висновок, зареєстрований в Адміністрації Державної служби спеціального зв'язку та захисту інформації України щодо відповідності вимогам нормативних документів системи технічного захисту інформації в Україні, сукупність яких визначається

функціональним профілем: КА-2, ЦА-1, ЦВ-1, ЦО-1, ДС-1, ДЗ-1, ДВ-1, ДР-1, НР-2, НИ-2, НО-1, НЦ-1, НТ-2, НК-1, НВ-1 з рівнем довіри не нижче ніж Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

Обов'язкове мають бути надані:

- оригінал листа авторизації від виробника про можливість постачання учасником продуктів антивірусного ПЗ в даних торгах.
- оригінал листа від виробника про можливість надання технічної підтримки антивірусного ПЗ, яке є предметом цієї закупівлі.
- нотаріально завірена копія експертного висновку Адміністрації Державної служби спеціального зв'язку та захисту інформації України (дійсний на момент розкриття пропозицій, в строк поставки товарів або надання послуг).

Вимоги до функціональних можливостей антивірусного ліцензійного програмного забезпечення наведені в таблиці:

Характеристика	**Вимоги**
Антивірусний захист	Сканування при доступі (т.з. On-Access) файлів, що зчитуються, записуються та їх тіньових копій Сканування за вимогою користувача або заплановане на консолі керування (т.з. On-Demand) Зберігання інформації з минулої перевірки та використання кешу для прискорення сканування Використання хмарного аналізу репутації контрольної суми файлу (Опціонально) можливість використання локальної «хмари» що міститиме інформації лише про ті вразливості, які були знешкоджені в інфраструктурі підприємства, автономно без передачі будь-якої інформації на сервери виробника антивірусного захисту Можливість блокування потенційно небезпечних активностей не залежно від результатів сигнатурного та хмарного аналізів Детектування шпигунського та небажаного ПЗ Можливість створення списків виключень та т.з. «чорних списків» додатків які не є вірусами Захист від широко спектру загроз (worm, Trojan, locker, cryptor, rootkit) та цілеспрямованих атак (опціонально) Перевірка активного наповнення Web сторінок Перевірка поштових повідомлень та приєднань (Опціонально) можливість статичного та динамічного аналізу коду для упередження зараження цілеспрямованими загрозами або невідомими досі вірусними додатками Перевірка архівних файлів Блокування спроб запуску додатків та скриптів з каталогів тимчасових файлів Блокування спроб реєстрації додатків як служб Блокування спроб ПЗ додати себе у список автозапуску Можливість антивірусного та анти-спам захисту поштових серверів MS Exchange та Lotus Можливість захисту налаштувань антивірусного модулю паролем (окремих або усіх) Можливість автоматичного відновлення роботи захисних модулів якщо вони були призупинені користувачем з дозволу оператора

	консолі
Консоль керування	Повинна забезпечувати наступний функціонал: Формування списку систем за групами, як в ручному режимі так і синхронізації структури служби каталогів Розгортання модулів захисту в автоматичному та в ручному режимі Підтримка розгорнутих систем в актуальному стані (оновлення ПЗ, синхронізація політик) Контроль стану кінцевих точок в режимі реального часу (за наявності мережевого з'єднання) Підтримка мінімум трьох гілок пакетів (поточний, попередній, випробування) Автоматичне сортування систем за їх типом, апаратними ресурсами та іншими властивостями Побудова графіків, діаграм, звітів та інформаційних шкал за даними з кінцевих точок Побудова розгалуженої деревовидної структури дзеркал головного репозиторію з підтримкою мережевих каталогів, Web або FTP джерел оновлення Можливість призначати різні політики (налаштування) на рівні окремих систем та груп систем Вбудований механізм планування задач по розгортанню, оновленню та супроводу модулів захисту Можливість вибіркового виконання завдань на рівні структури компанії, групи або підгрупи Зберігати каталог політик з можливістю їх копіювання та пере налаштування під певні групи Обов'язковий лог аудиту дій операторів консолі Рольова модель доступу з можливістю формування певних шаблонів рівня доступу Автентифікація по локальній базі користувачів та можливість використання облікових записів AD Прийом та обробку журналів подій із кінцевих точок Фіксований інтервал комунікації кінцевих точок із консоллю керування Можливість ініціалізації позапланового сеансу зв'язку як з боку консолі так і з кінцевої точки Можливість налаштування інтервалу комунікації на рівні окремих кінцевих точок та груп (Опціонально) Розширення захисту за допомогою прозорої інтеграції засобів шифрування дисків та файлів/каталогів і зовнішніх носіїв (Опціонально) Розширення захисту за допомогою прозорої інтеграції засобів мережевого захисту (IPS, NGF) (Опціонально) Розширення захисту за допомогою прозорої інтеграції засобів розширеного захисту електроної пошти (антивірус, анти-спам, шифрування пошти) (Опціонально) Розширення захисту за допомогою прозорої інтеграції засобів розширенного захисту Web (антивірус, сканування скриптів, Web-фльтрація) (Опціонально) Розширення захисту за допомогою прозорої інтеграції засобів оцінки ризиків (Опціонально) Розширення захисту за допомогою прозорої

	інтеграції засобів підтвердження відповідності стандартів (Опціонально) Розширення захисту за допомогою прозорої інтеграції засобів контролю вразливостей (Опціонально) Розширення захисту за допомогою прозорої інтеграції захисту додаткових модулів мережевого DLP Можливість масштабування з урахуванням збільшення кількості кінцевих точок та розширення захисного функціоналу Можливість синхронізації політик та трансферу керованих кінцевих точок між двома консолями керування Можливість вбудованого резервного копіювання бази даних
Контроль мережевих з'єднань	Мережевий брандмауер Режим навчання, автоматичний режим роботи Вбудовані правила для поширеного ПЗ (ОС, офісні та інтернет додатки) (Опціонально) система упередження вторгнень (Опціонально) аналіз мережевих пакетів, перевірка відповідності RFC, виявлення аномалій (Опціонально) контроль пам'яті запущених процесів (Опціонально) можливість захисту систем, які з різних причин не часто отримують оновлення ОС та ПЗ
Веб-контроль	Можливість перевірки репутації URL Виявлення сайтів із небезпечним наповненням Можливість блокування доступу до жерел певної категорії Можливість дозволу доступу до URL але блокування можливості завантажити файл(и) Створення т.з. «чорних списків» URL не залежно від їх репутації (Опціонально) можливість синхронізації категорій URL із шлюзом веб-безпеки (Опціонально) перевірка захищеного трафіку (SSL сесії) (Опціонально) розширена перевірка активного вмісту веб-сторінок (Опціонально) Розмежування доступу до різних категорій URL по групам користувачів (Опціонально) примусова антивірусна перевірка файлів, що завантажуються (Опціонально) можливість перехоплення Web трафіку по протоколу ICAP на DLP систему
Контроль додатків	Упередження блокування редактору реєстру та командного рядка Блокування спроб перехоплення системних служб Упередження зупинки модулів захисту Блокування запуску додатків та/або сценаріїв з каталогів тимчасових файлів Захист налаштувань бравзерів Блокування спроб реєстрації додатків в якості системних служб Блокування спроб реєстрації додатків у списку автозавантаження Запобігання створення запускних файлів у системних каталогах Блокування запуску додатків без цифрового підпису Блокування реєстрації нових APPID, TYPELIB та CLSID (Опціонально) можливість формування т.з. «білих списків» додатків (Опціонально) можливість запиту на дозвіл виконання забороненого додатка

Контроль пристроїв	Моніторинг, примусове блокування або переведення в режим «readonly» зовнішніх носіїв (USB) Моніторинг та/або блокування зовнішніх пристроїв на кшталт модемів, плат розширень та ін. Формування «білих» та «чорних» списків пристроїв за багатьма параметрами (SN, PID&VID, ID) Контроль пристроїв на рівні шини Можливість перевірки змісту документів, які користувач зберігає на зовнішній носій Можливість блокування спроб запису/копіювання документів на зовнішні носії, що збігаються з цифровими відбитками або містять слова, словосполучення вказані замовником Застосування правил до локальних та доменних користувачів Можливість тимчасового обходу блокування (дозволу роботи з певними пристроями) Ведення окремого журналу інцидентів пов'язаних із пристроями та носіями Можливість різної поведінки системи в залежності від стану системи (online / offline) Можливість перехоплення тіньових копій файлів, які користувач копіює або записує на зовнішній носій (Опціонально) Можливість інтеграції модулю контролю пристроїв із модулем вибіркового шифрування файлів з метою забезпечення можливості шифрування файлів перед записом на носії (Опціонально) Можливість інтеграції модулю контролю пристроїв із модулем вибіркового шифрування файлів з метою створення криптографічних контейнерів на зовнішніх носіях (Опціонально) Можливість миттєвого розширення функціоналу до повноцінного DLP для кінцевих точок з можливістю контролю друку, буферу обміну, Web, Email та іншої активності користувачів (Опціонально) Інтеграція з сервісом MS RMS
Інші можливості	Наявність розширень для поширених додатків типу IE, FF, MS Outlook Підтримка серверів терміналів (Опціонально) інвентаризація встановленого ПЗ з можливістю формування «чорних списків» Можливість тимчасового увімкнення максимального захисту на випадок вірусної епідемії Можливість контролювати параметру карантину (каталог збереження та період) Можливість повністю приховати графічний інтерфейс від користувача
Оновлення	Можливість оновлення встановлених захисних модулів з різних джерел (формування списку): консоль керування, дзеркало репозитарію консолі керування або ж із серверів виробника Можливість налаштування вибіркових параметрів оновлення для різних груп систем Можливість встановлення оновлень антивірусних баз у off-line режимі на консоль керування та на кінцевих точках Файли оновлень мають бути захищені цифровим підписом виробника, при оновлені консоль та модулі захисту мають

	обов'язково перевіряти цілісність оновлень та їх легітимність Можливість створення дзеркал головного репозитарію у віддалених філіалах Можливість оптимізованого кешування на дзеркалах, коли дзеркало містить лише ті модулі, які використовуються на системах віддаленого філіалу
Звітність	Локальне зберігання журналів подій захисних модулів Можливість налаштування об'єму та критичності подій які будуть передаватися на консоль керування Централізований збір журналів (логів) з усіх кінцевих точок, які захищаються Можливість побудови інформаційних шкал за даними отриманими з кінцевих точок Можливість конструювання звіту з підготовлених запитів Можливість автоматичного створення звітів та їх експорту або відправки по електронній пошті
Підтримка операційних систем	Windows: XP SP3 Professional x32/x64 (SP2) Vista SP2 x32 7 x32/x64 8/8.1 x32/x64 Server 2003 SP2/R2 Server 2008 SP2 Server 2008 R2 Server 2012 Apple: Mac OS X Mavericks 10.9 та вище Mac OS X Mountain Lion 10.8 та вище Mac OS X Lion 10.7 та вище Mac OS X Snow Leopard 10.6 та вище Mac OS X Leopard 10.5 та вище NIX: FreeBSD 6 та вище HP-UX 11 та вище IBM AIX 5 та вище Linux deb та rpm kernel 2.4 та вище Solaris 8 та вище

4.3. Місце поставки товарів або надання послуг.
вул. Кутузова, 18/9, м. Київ-133, 01601
4.4. Строк поставки товарів або надання послуг. ***Не більше 10 (десяти) календарних днів з дати підписання Договору.***
5. Основні умови договору.

Предмет договору

Виконавець зобов'язується надати послуги щодо видання ліцензії на право користування програмним забезпеченням (код 58.29.5 згідно з ДК 016:2010) (послуги з постачання антивірусного ліцензійного програмного забезпечення).

Обсяги закупівлі послуг можуть бути зменшені залежно від реального фінансування видатків.

Якість послуг

Виконавець гарантує, що безперервний простій в наданні послуг не повинен перевищувати 8 годин.

Виконавець повинен надати Замовнику послуги, вчасно та належної якості, згідно з умовами, зазначеними у запиті цінових пропозицій.

<u>Ціна договору</u>

Ціна договору становить _____.

Ціна договору дорівнює ціні пропозиції переможця запиту цінових пропозицій.

Ціна договору може бути зменшена за взаємною згодою сторін.

<u>Порядок здійснення оплати</u>

Оплата за надані Послуги здійснюється протягом 10 (десяти) робочих днів після підписання Акту приймання-передачі програмного забезпечення у безготівковій формі шляхом перерахування коштів в національній валюті України з рахунку Замовника на рахунок Виконавця за умови наявності бюджетного фінансування Замовника.

У разі відсутності фінансування з Державного бюджету України Замовник не несе відповідальності за прострочення оплати, але зобов'язується оплатити надані послуги відразу після надходження відповідного фінансування з Державного бюджету України.

У разі, якщо реальні обсяги фінансування в 2015 році, передбачені в кошторисі Замовника, будуть зменшені по відношенню до запланованих (на яких базується вартість цього Договору), Сторони повинні будуть переглянути умови Договору з метою приведення вартості Договору у відповідність до фактичних обсягів фінансування.

Розрахунки за договором про закупівлю здійснюються через Державну казначейську службу України.

<u>Поставка товарів</u>

Строк поставки товарів або надання послуг: не більше 10 (десяти) календарних днів з дати підписання Договору.

<u>Місце надання послуг</u>

01601, м. Київ-133, вул. Кутузова, 18/9.

6. Строк дії цінових пропозицій. ***120 календарних днів з дня відкриття***

7. Подання цінових пропозицій.

7.1. Місце та спосіб подання. ***вул. Кутузова, 18/9, к.106, м. Київ-133, 01601, особисто***

7.2. Строк. ***З дня оприлюднення запиту цінових пропозицій на веб-порталі Уповноваженого органу до 10-00 09.09.2015 р.***

8. Розкриття цінових пропозицій.

8.1. Місце. ***вул. Кутузова, 18/9, к.106, м. Київ-133, 01601***

8.2. Дата. ***09.09.2015***

8.3. Час. ***об 11-00***

9. Додаткова інформація.

Учасник визначає ціни на послуги, з урахуванням усіх своїх витрат, податків і зборів, що сплачуються або мають бути сплачені. До розрахунку ціни входять усі види послуг, у тому числі й ті, які доручатимуться для виконання третім особам. Не врахована Учасником вартість окремих послуг не сплачується Замовником окремо, а витрати на їх виконання вважаються врахованими у загальній ціні пропозиції.

Цінова пропозиція подається у письмовій формі згідно з **ДОДАТКОМ.**

Цінова пропозиція подається особисто в письмовій формі за підписом Учасника, прошита, пронумерована та скріплена печаткою*, у запечатаному конверті Комітету з конкурсних торгів апарату Фонду державного майна України за адресою: ***01601, м. Київ 133, вул. Кутузова, 18/9, к. 106 (тел. 200-35-76) до 10:00, 09.09.2015 року.***

На конверті зазначають зворотну адресу, назву учасника і позначки "***На конкурс із закупівлі послуг щодо видання ліцензії на право користування програмним забезпеченням (код 58.29.5 згідно з ДК 016:2010) (послуги з постачання антивірусного ліцензійного програмного забезпечення) та "Не відкривати до 11:00, 09.09.2015 року".***

Цінова пропозиція Учасника, що отримана Замовником після закінчення строку її подання та не за зазначеною адресою, не розкривається і повертається Учаснику, що її надав.

Учасник запиту повинен надати:

- довідку у довільній формі про підтвердження відсутності підстав для відмови учаснику в участі у процедурі закупівлі, а саме:

1) він має незаперечні докази того, що учасник пропонує, дає або погоджується дати прямо чи опосередковано будь-якій посадовій особі замовника, іншого державного органу винагороду в будь-якій формі (пропозиція щодо найму на роботу, цінна річ, послуга тощо) з метою вплинути на прийняття рішення щодо визначення переможця процедури закупівлі або застосування замовником певної процедури закупівлі;

2) службову (посадову) особу учасника, яку уповноважено учасником представляти його інтереси під час проведення процедури закупівлі, фізичну особу, яка є учасником, було притягнуто згідно із законом до відповідальності за вчинення у сфері державних закупівель корупційного правопорушення;

3) суб'єкт господарювання (учасник) протягом останніх трьох років притягувався до відповідальності за порушення, передбачене пунктом 4 частини другої статті 6, пунктом 1 статті 50 Закону України "Про захист економічної конкуренції", у вигляді вчинення антиконкурентних узгоджених дій, які стосуються спотворення результатів торгів (тендерів);

4) фізична особа, яка є учасником, була засуджена за злочин, вчинений з корисливих мотивів, судимість з якої не знято або не погашено у встановленому законом порядку;

5) службова (посадова) особа учасника, яку уповноважено учасником представляти його інтереси під час проведення процедури закупівлі, була засуджена за злочин, вчинений з корисливих мотивів, судимість з якої не знято або не погашено у встановленому законом порядку;

6) пропозиція конкурсних торгів подана учасником процедури закупівлі, який є пов'язаною особою з іншими учасниками процедури закупівлі та/або з членом (членами) комітету з конкурсних торгів замовника;

7) учасник визнаний у встановленому законом порядку банкрутом та відносно нього відкрита ліквідаційна процедура;

8) інформація про те, що відомості про юридичну особу, яка є учасником, не вносились до Єдиного державного реєстру осіб, які вчинили корупційні або пов'язані з корупцією правопорушення;

9) інформація щодо наявності антикорупційної програми та уповноваженого з антикорупційної програми юридичної особи у випадку, коли вони є обов'язковими відповідно до закону, із наданням копії антикорупційної програми юридичної особи та копії наказу про призначення уповноваженого з антикорупційної програми юридичної особи, або інформація про відсутність антикорупційної програми та уповноваженого з антикорупційної програми юридичної особи у випадку, коли вони не є обов'язковими відповідно до закону;

- копію статутних документів (Статуту, Установчого договору) Учасника (для юридичних осіб);

- довідку (або копію довідки) з податкової інспекції про відсутність заборгованості за обов'язковими платежами до бюджету**, дійсну на момент розкриття цінових пропозицій;**

- довідку (або копію довідки) відповідного органу про відсутність рішення про порушення проти суб'єкта господарювання справи про банкрутство чи визнання його в установленому порядку банкрутом, видану не пізніше 30-денної давнини відносно фактичної дати розкриття пропозиції;

- документ(и) (або копія документу(ів)), що підтверджує(ють) правомочність представника Учасника на укладення договору про закупівлю (виписка з протоколу засновників, наказ про призначення, довіреність, доручення або інший документ);

- документ(и) (або копія документу(ів)), що підтверджує(ють) повноваження посадової особи учасника процедури закупівлі щодо підпису документів пропозиції конкурсних торгів (виписка з протоколу засновників, наказ про призначення, довіреність, доручення або інший документ).

Всі копії та довідки Учасника повинні бути належним чином посвідченими, тобто підписані уповноваженою особою Учасника (для юридичних осіб підпис уповноваженої особи Учасника засвідчується власною печаткою* Учасника).

У випадку присутності Вас або Вашого представника під час розкриття при собі необхідно мати:

- *якщо Учасником запиту є фізична особа, то вона повинна мати при собі оригінал документа, що засвідчує його особу;*
- *якщо Учасником запиту виступає юридична особа, яку представляє керівник, він повинен надати завірені копії документів, що підтверджують його повноваження, та мати при собі оригінал документа, що засвідчує його особу;*
- *у разі якщо Учасника представляє інша особа, їй необхідно надати довіреність на представництво інтересів Учасника, підпис документів, та мати при собі оригінал документа, що засвідчує її особу.*

ДОДАТОК

Форма
цінової пропозиції
(*форма, яка подається Учасником на фірмовому бланку*)

Ми, (повне найменування та адреса, місцезнаходження Учасника), надаємо свою пропозицію щодо предмету закупівлі ***послуги щодо видання ліцензії на право користування програмним забезпеченням (код 58.29.5 згідно з ДК 016:2010) (послуги з постачання антивірусного ліцензійного програмного забезпечення)*** згідно з вимогами Замовника торгів, зазначених у його запиті, на загальну суму:

Загальна вартість пропозиції:_____ (з урахуванням ПДВ) (грн.)
(прописом)

Вивчивши запит цінових пропозицій та основні вимоги на виконання зазначеного вище, ми, уповноважені на підписання Договору, маємо можливість та погоджуємося виконати вимоги Замовника.

1. Ми погоджуємося дотримуватися умов цієї пропозиції протягом 120 календарних днів з дня її відкриття. Наша пропозиція буде обов'язковою для нас до закінчення зазначеного терміну.
2. Ми погоджуємося з основними умовами Договору.
3. Якщо наша пропозиція буде акцептована, ми беремо на себе зобов'язання на підписання Договору відповідно до основних умов договору, зазначених у запиті, ***у строк не раніше ніж через три робочі дні з дня оприлюднення на веб-порталі Уповноваженого органу повідомлення про акцепт цінової пропозиції, але не пізніше ніж через 14 днів з дня визначення переможця,*** і виконати всі умови, передбачені Договором.

Посада, прізвище, ініціали, підпис уповноваженої особи Учасника, (для юридичних осіб підпис уповноваженої особи Учасника засвідчується власною печаткою* Учасника)_____

* Ця вимога не стосується учасників, які здійснюють діяльність без печатки згідно з чинним законодавством.