Приложение № 2
към рамков договор № МС-117/09.10.2024 г.

ЗАЯВКА по Рамков договор № МС-117 от 09.10.2024 г. **(№ ПО-16-3093/09.10.2024 г. на ИО АД)**	☒
ЗАЯВКА по Рамков договор № МС-117 от 09.10.2024 г. **(№ ПО-16-3093/09.10.2024 г. на ИО АД)** **(актуализирана)**	☐ [1]

Позиция от ПГ-2025 г.:	*№ по ред от ПГ*	*6*
Описание на проект съгласно ПГ:	*Обследване на ИСУН*	
CPV код	*72225000-8*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	МЕУ-19804/19.12.2025 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*	***15 000,00 лв.***
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Еднократно, след подписването от страните на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършените дейности и издадена фактура.*
Плащане с акредитив ДА/НЕ	*ДА* *При невъзможност до края на бюджетната година дейността да бъде изпълнена цялостно или частично, Бенефициерът ще открие сметка за разплащане на дължимите суми (неотменяем акредитив), която ще покрива срока за извършване на услугата*
Документи за плащане с акредитив	*Документи за банката за усвояване на средствата – фактура, издадена от Изпълнителя, подписана от оторизираните представители на Администрацията на Министерския съвет и подписан приемно-предавателен протокол по чл.6 от договора за приемане на съответния етап*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*До 20 дни след подписване на заявката.*
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)*	*Еднократно, с подписването от страните на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършените дейности*
Приложения: (*напр: технически параметри, образци на отчетни*	*Технически параметри.*

[1] Отбелязва се в случай че заявката е актуализирана

документи)	
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 ВЪЗЛОЖИТЕЛЯ:	*Подпис:*
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

ТЕХНИЧЕСКИ ПАРАМЕТРИ

Извършване на обследване и първоначални разширени одити на използваните централизирани информационните системи ИСУН и подготовка на документация от правила

Изпълнителят трябва да използва методологии и добри практики в киберсигурността при анализ, оценка и тестове за проникване (penetration testing) на уеб базирани платформи.

Изпълнителя трябва да се базира на изискванията на Закона за киберсигурност, Наредбата за минималните изисквания за мрежова и информационна сигурност, както и на методологии OWASP (Open Web Application Security Project) и/или MITRE.

I. Методология OWASP:

1. Инжектиране (Injection)

Възниква, когато недоверени данни се използват в интерпретатор за изпълнение на команди, което води до изпълнение на неочаквани и вредни команди в базата данни или други системи. Пример: SQL инжекции.

2. Неизправно удостоверяване (Broken Authentication)

Възниква, когато системите за удостоверяване не осигуряват защита срещу атаки и позволяват неоторизирани достъпи до чувствителни данни или услуги.

3. **Излагане на чувствителна информация (Sensitive Data Exposure)**

Когато чувствителни данни като пароли, финансови данни и лична информация не се обработват или съхраняват правилно, което може да доведе до тяхното излагане.

4. **Недостатъчно разрешение (Broken Access Control)**

Когато системата не ограничава правилно достъпа на потребители до ресурси или данни, които не им принадлежат.

5. **Неправилна конфигурация на сигурността (Security Misconfiguration)**

Възниква, когато приложенията или сървърите не са конфигурирани правилно по отношение на сигурността, като например използване на стандартни настройки, неактивирани защитни функции или публично достъпни файлове.

6. **Използване на неактуален компонент (Using Components with Known Vulnerabilities)**

Използването на библиотеки или компоненти, които съдържат уязвимости, може да изложи приложенията на атаки.

7. **Недостатъчна защита срещу Cross-Site Scripting (XSS)**

Когато приложенията не проверяват правилно входните данни от потребителите, което може да позволи на нападатели да изпълняват злонамерен JavaScript код в браузъра на жертвата.

8. **Недостатъчна защита срещу Cross-Site Request Forgery (CSRF)**

Атака, при която нападателят принуждава потребителя да извърши неоторизирано действие на уебсайт, на който е аутентифициран.

9. **Използване на небезопасни API-та (Using Insecure APIs)**

Възниква, когато приложенията използват API-та, които не осигуряват необходимото ниво на защита или не са достатъчно проверени.

10. **Недостатъчна защита срещу несанкциониран достъп (Insufficient Logging & Monitoring)**

Липсата на необходимото логване и мониторинг, което предотвратява откритията на неоторизирани действия и атаки, може да доведе до неуспешно предотвратяване на пробиви.

Анализ, оценка и пенетрейшън тестове на уеб базирани платформи по методологията MITRE

II. Методология MITRE за Пенетрейшън тестове:

1. **Идентифициране на заплахи и цели**

Използването на MITRE ATT&CK рамката за идентифициране на различни видове заплахи, насочени към уеб платформи, както и потенциалните цели, които могат да бъдат компрометирани по време на тестовете.

2. **Разузнаване (Reconnaissance)**

- Преглед на публично достъпни данни за уеб платформата, включително DNS записи, IP адреси и публични акаунти.
- Събиране на информация за уязвимости на базата на исторически атаки, използвайки техники като "Fingerprinting" (идентифициране на софтуерни компоненти).

3. **Идентифициране на уязвимости (Vulnerability Identification)**

- Анализ на уеб платформата за известни уязвимости, които могат да бъдат експлоатирани.
- Използване на техники от MITRE ATT&CK като **Scripting**, **Exploitation for Privilege Escalation** или **SQL Injection**.
- Провеждане на автоматизирани и ръчни тестове с инструменти като Burp Suite, OWASP ZAP и Nessus за откриване на уязвимости.

4. **Експлоатация на уязвимости (Exploitation)**

- Използване на различни техники от MITRE за експлоатация на откритите уязвимости:
  - **Command and Control** – манипулиране на уеб сървъри и услуги.
  - **Web Shell** – инсталиране на уеб шелове за отдалечен достъп.
  - **Privilege Escalation** – увеличаване на правата на потребителя чрез уязвимости като инжекции или неконтролируеми API-та.

5. **Управление на пристъпи (Post-Exploitation)**

След като уязвимостта бъде експлоатирана, тестването преминава в етапа на управление на достъп до системата:

- Използване на **Lateral Movement** за преминаване през други части на платформата.
- Повишаване на привилегиите чрез техники като **T1071** (Application Layer Protocols).
- Установяване на стабилни бекдор канали.

6. **Докладване и препоръки**
   - Оценка на рисковете от откритите уязвимости.
   - Препоръки за защита, включително конфигурации за сигурност, стратегии за мониторинг и подобрения в методите за удостоверяван
7. **Представяне на детайлен доклад** за напредъка на теста, обяснение на откритите уязвимости и предложения за тяхното коригиране.

III. Текущо състояние и обхват на провежданите тестове:

Таблица 1

№	Система	Описание
1	3 броя App Server	Application servers, работещи в режим NLB (Network Load Balancer)
2	1 брой App Server	Application server за вътрешната среда на системата
3	1 брой public server	Сървър предоставящ публична информация по проектите, налични в ИСУН
4	2 броя database server	Сървър за бази данни
5	1 брой Redis	Redis Server
6	1 брой gate server	системата ползва необходимите за работа услуги от Държавния хибриден частен облак, вкл. и _системите за защита на данните.

IV. Основни задачи за изпълнение

1. **Анализ на текущото състояние и оценка на системите описани в Таблица 1**

1.1. Планиране на обхвата и времевата рамка на проекта с клиента (Специфики, изисквания)

1.1.1. При сключване на договора в подготвителната фаза, Изпълнителят трябва да предостави подробен списък с инструментите, които ще бъдат използвани по време на оценката, включително софтуерни и хардуерни инструменти (напр. vulnerability scanners, network sniffers, penetration testing frameworks) и информация за лицензите им (тип, валидност, доставчик).

1.1.2. В рамките на тази фаза, трябва да се извършат подготвителни дейности преди тестване, които да включват: създаване на пълни резервни копия на всички релевантни компоненти на инфраструктурата; проверка на целостта на архивираните конфигурации и възстановимостта на резервните копия; архивиране на конфигурациите на всички мрежови устройства (рутери, суичове, защитни стени).

1.2. Извършване на ИКТ (информационни и комуникационни технологии) одит от гледна точка на информационната сигурност на системите описани в Таблица 1

1.2.1. Общ преглед и оценка на системите в Таблица 1

1.2.1.1. Анализ на архитектурата и дизайна

1.2.1.2. Верификация и валидация на изходния код, процедури и техническа документация

1.2.1.3. Преглед на използваните механизми за автентикация на крайните потребители на системите, защита на информацията, пароли и съхранение

1.2.1.4. Преглед на механизмите за достъп до базата данни

1.2.1.5. Преглед за наличие и управление на журнални файлове (логове)

1.2.1.6. Преглед на управлението на криптографски механизми, алгоритми, ключове и контроли

1.2.1.7. Оценка на евентуални уязвимости на системите описани в Таблица 1

1.2.1.7.1. Изготвяне на документация и доклад

1.2.2. Преглед и оценка на сигурността на базата данни на системите описани в Таблица 1, както и системата за управление на базите данни (СУБД)

1.2.2.1. Оценка на използваните административни акаунти

1.2.2.2. Възможности за отдалечен достъп до базите данни

1.2.2.3. Оценка на евентуални уязвимости

1.2.2.3.1. Изготвяне на документация и доклад

1.2.3. Преглед и оценка на сигурността на сървърите свързани с работата на информационните системи описани в Таблица 1

1.2.3.1. Преглед и обща оценка на сигурността на сървърите и предоставените от тях услуги

1.2.3.2. Преглед на сигурността на операционните системи -

1.2.3.3. Преглед на сигурността на използвания уеб сървър -

1.2.3.4. Преглед на използваните механизми за автентикация, защита на информацията, пароли и съхранение

1.2.3.5. Оценка на евентуални уязвимости

1.2.3.5.1. Документация и доклад

1.2.4. Анализ на използваните механизми за сигурност в комуникационната среда обслужваща информационните системите описани в Таблица 1

1.2.4.1. Преглед и обща оценка на сигурността на мрежовата и комуникационна инфраструктура

1.2.4.2. Анализ на настройките на защитните стени

1.2.4.3. Анализ на възможността за несанкциониран достъп

1.2.4.4. Документация и доклад

1.2.5. Изпитване чрез тестове за неоторизиран пробив (penetration test) на информационна система описани в Таблица 1 и използваната система за управление на базите данни (СУБД) в контролирана среда

1.2.5.1. Извършване на сканиране (Vulnerability Assessment) и уязвимости и потенциални заплахи за сигурността на информацията на системата -

1.2.5.2. Преглед и обща оценка на сорс кода на информационните системи описани в Таблица 1 от гледна точка защита на системата от неоторизиран достъп (backdoors, SQL injection и т.н), както и други аспекти от информационната сигурност

1.2.5.3. Анализ и оценка на евентуални уязвимости

1.2.5.4. Документация и доклад

1.2.6. Извършване на независима експертиза за съответствие на разработената информационните системи описани в Таблица 1 с Техническите спецификации и НМИМИС

1.2.6.1. Констатиране на несъответствия с техническите спецификации

1.2.6.2. Преглед и обща оценка на функционалностите на информационните системи от гледна точка на сигурността, безотказността, резервираността и надеждността на системите;

1.2.6.3. Преглед и обща оценка на модулите на информационните системи

1.2.6.4. Преглед и обща оценка на обезпечаване на работните процеси

1.2.6.5. Документация и доклад

1.2.7. Изпълнение на процедура за предаване и унищожаване от страна на Изпълнителя на всички събрани артефакти по време на тестването

1.2.8. Извършване на независима експертиза за съответствие на информационните системи описани в Таблица 1 с общоприетите изисквания за качество на една информационна система

1.2.8.1. Проверка на: бързина, удобство, бърза връзка за свързване с функционалностите, сигурност при ползването, опазване на данните, наличие на системи за защита, дублиране и опазване на информацията, backup

1.2.8.2. Наличие на ръководство за експлоатация, последваща поддръжка, актуализация на софтуера, закърпване на т.нар. „пач“, осигуряване на непрекъсната 24-часова връзка, 7 дни в седмицата, реакция при нужда и други общоприети изисквания

1.2.8.3. Документация и доклад

2. Изпълнителят следва да изготви проект на Правила съгласно чл.5, ал. 1, точки 6 и 7 от Наредбата за минималните изисквания за мрежова и информационна сигурност.

Всички резултати от тестовете да бъдат придружени от сурови данни (напр. scan outputs, command logs, traffic captures), които да подкрепят прозрачността и да позволяват независима проверка.