<table>
<tr><td colspan="3">ЗАЯВКА по Договор № ДОГ-100 от 19.12.2023 г.
(вх. № ПО-16-3466/19.12.2023 г. на ИО АД)</td><td>☒</td></tr>
<tr><td colspan="3">ЗАЯВКА (актуализирана)</td><td>☐ [1]</td></tr>
<tr><td>Позиция от ПГ-2024 г.</td><td>№ по ред от ПГ</td><td colspan="2">6.2</td></tr>
<tr><td>Описание на дейност/проект съгласно ПГ:</td><td colspan="3">Дейности, които осигуряват изпълнението на услугите по системна интеграция - проект на части</td></tr>
<tr><td colspan="2">CPV код</td><td colspan="2">72800000-8 - Услуги по компютърен одит и компютърно тестване</td></tr>
<tr><td colspan="2">Част 3</td><td colspan="2">Извършване на технически одит за изясняване на възникнал инцидент в инфраструктурата на Министерство на финансите</td></tr>
<tr><td colspan="2">Изискване за достъп до класифицирана информация ДА/НЕ</td><td colspan="2">НЕ</td></tr>
<tr><td colspan="2" rowspan="2">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</td><td>Стойност на част 3 от проект 6.2 за 2024 г.:</td><td>Стойност с натрупване за възложените части по проект 6.2 за 2024 г.</td><td>Стойност на проект 6.2 за 2024г. (съгл. ПГ-2024 г., в. 1.0)</td></tr>
<tr><td>8 640 лв.</td><td>Общо 45 990,00 лв.
Част 1 – 10 500,00 лв.
Част 2 – 26 850,00 лв.
Част 3 – 8 640 лв.</td><td>348 500,00 лв.</td></tr>
<tr><td colspan="2">Начин на плащане:
(еднократно, на части, периодично, авансово или др.)</td><td colspan="2">Еднократно, при предоставянето на:
• Протокол за изпълнение на проект по чл. 9, ал. 1 от Договора, с приложени:
○ Финансова справка;
○ Технически доклад за изясняване на възникнал инцидент в информационната и комуникационна инфраструктура.
• Фактура.</td></tr>
<tr><td colspan="2">Плащане с акредитив или авансово
ДА/НЕ</td><td colspan="2">Не е приложимо</td></tr>
<tr><td colspan="2">Документи за плащане с акредитив или авансово</td><td colspan="2">Не е приложимо</td></tr>
<tr><td colspan="2">Срок на изпълнение: (от дата – до дата или в месеци, ако не е обвързан с конкретна дата)</td><td colspan="2">Съгласно чл. 1, ал. 7, изр. 3 от Договора, проектът се изпълнява от 05.03.2024 г.;
Срок за изпълнение - 3 работни дни</td></tr>
<tr><td colspan="2">Гаранционен срок: (от дата – до дата или в месеци, ако не е обвързан с конкретна дата)</td><td colspan="2">Не е приложимо</td></tr>
<tr><td colspan="2">Отчитане: (периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)</td><td colspan="2">Еднократно, съгласно приложените ТП</td></tr>
<tr><td colspan="2">Приложения: (напр: технически параметри, образци на отчетни документи)</td><td colspan="2">Технически параметри (ТП) за извършване на технически одит за изясняване на инцидент в инфраструктурата на Министерство на финансите</td></tr>
<tr><td colspan="4">Настоящата заявка да се изпълни при условията на приложените Технически параметри.</td></tr>
<tr><td colspan="4">ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:</td></tr>
<tr><td colspan="2">Координатор по заявката:</td><td colspan="2"></td></tr>
</table>

[1] Отбелязва се в случай че заявката е актуализирана

Ръководител на проект/дейност по заявката (напр: представител на дирекцията – Заявител):	
ЗАЯВКАТА е ОДОБРЕНА ОТ:	
Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:	
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:	
Координатор от „Информационно обслужване“ АД по заявката и Ръководител по изпълнението на Договора от „Информационно обслужване“ АД	
Ръководител на проект/дейност по заявката	

РЕПУБЛИКА БЪЛГАРИЯ

МИНИСТЕРСТВО НА ФИНАНСИТЕ

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА ИЗВЪРШВАНЕ НА ТЕХНИЧЕСКИ ОДИТ ЗА ИЗЯСНЯВАНЕ НА ИНЦИДЕНТ В ИНФРАСТРУКТУРАТА НА МИНИСТЕРСТВО НА ФИНАНСИТЕ

м. март, 2024 г.

1. **Съществуващо положение**

В изпълнение на проект „4.1 Осигуряване на управлението на събития и сигурността на информацията и Cloudflare "Pro" за нуждите на МФ - ПРЕХОДЕН ПРОЕКТ“ от План-графика за 2024 г. към договор №ДОГ-100/2023 г., на 27.02.2024 г. в 4.40 ч. сутринта са активирани аларми в Qradar, регистрирани като „Possible Local Worm Detected“ за анормално поведение, приличащо на червей в мрежата на Министерство на финансите (МФ), в частност – на Изпълнителна агенция „Одит на средствата от европейския съюз“ (ИАОСЕС).

Анализът на алармите потвърждава наличието на инцидент по мрежова и информационна сигурност, във връзка с което Служителят по мрежова и информационна сигурност (СМИС) в МФ информира CERT България, чрез подаване на сигнал, регистриран под № rtir.govcert.bg #27116/28.02.2024 г.

На 28.02.2024 г. до директора на дирекция „Информационни системи“ в МФ постъпва доклад от центъра за информационна сигурност на „Информационно обслужване“ АД (Security Operation Center - SOC), чрез г-н Симеон Кърцелянски, ръководител отдел „Оперативен център за киберсигурност“…..и ръководител на проект 4.1. Докладът съдържа първоначална информация за инцидента, възникнал на 27.02.2024 г.

Предприети са действия за смяна на паролите на всички потребители както от ИАОСЕС, така и от МФ. Организирано е сканиране с антивирусен софтуер на всички машини в двете ведомства.

На 04.03.2024 г. сутринта отново са активирани аларми в Qradar за регистрирано проникване в мрежата на ИАОСЕС, аналогично на инцидента от 27 февруари 2024 г.

На 05.03.2024 г. е изпратено писмо от главния секретар на МФ до председателя на Държавна агенция „Национална сигурност“ (ДАНС) с молба за оказване на експертно – техническа помощ и извършване на допълнителна проверка в инфраструктурата на ИАОСЕС и МФ.

2. **Цел**

Извършване на цялостно сканиране на информационно-комуникационната инфраструктура в МФ, в която се намира и инфраструктура на ИАОСЕС с цел изясняване на възникнал инцидент, анализ на резултатите от сканирането и даване на препоръки за предприемане на мерки (преправяне и/или добавяне на правила и политики) за повишаване на сигурността.

3. **Място на предоставяне на услугата**

Мястото на предоставяне на услугата е сградата на МФ, намираща се в гр. София, ул. „Г. С. Раковски“ № 102 и ул. „Славянска“ № 4.

4. **Изисквания към Изпълнението**

Предвид естеството на възникналия инцидент, изпълнението на проекта започва преди неговото официално възлагане, на 05.03.2024 г.

Проверката следва да се направи от SOC – екипа на системния интегратор на място.

5. **Изисквания към мрежовата и информационната сигурност**

Изпълнителят следва да осигури изпълнението съгласно Раздел IV от документа „Общи изисквания за изпълнение на проекти/дейности по системна интеграция“ към План-графика за 2024 г. и съгласно действащите правила за физически достъп до информационно-технологичните и комуникационни центрове на МФ.

6. **Дейности**

6.1. Цялостно сканиране на информационно - комуникационната инфраструктура в МФ и ИАОСЕС:

а) Събиране на логове от Domain Controllers
б) Събиране на логове от Exchange
в) Събиране на логове от Exchange web сървър (IIS логове)
г) Преглеждане и събиране на логове от web proxy
д) Преглеждане и събиране на логове на защитни стени
е) Преглеждане и събиране на логове With Secure
ж) Събиране на логове от Netwrix
з) Одитиране на активна директория
и) Събиране на мрежова комуникация (PCAP)

6.2. Анализ на получената информация и изготвяне на технически доклад за изясняване на възникнал инцидент, който съдържа описание на констатациите и дадени препоръки.

7. Отчитане и плащане

7.1. Отчетните документи по проекта, чиито образци са съгласно „Общи изисквания за изпълнение на проекти / дейности по системна интеграция“ към План-графика за 2024 г. са както следва:

а) Протокол за изпълнение на проект (Образец № 1);
б) Финансова справка (Образец № 2);
в) Технически доклад за изясняване на възникнал инцидент – предава се на ръководителя на проекта по електронна поща.

7.2. Плащането се извършва еднократно, на база приети отчетни документи по т. 7.1 и издадена фактура, одобрена от Възложителя.