MINISTERO DELLA DIFESA

SEGRETARIATO GENERALE DELLA DIFESA E DIREZIONE NAZIONALE DEGLI ARMAMENTI

DIREZIONE DEGLI ARMAMENTI NAVALI

II Reparto – SISTEMA NAVE

IV Divisione – PROPULSIONE ed ENERGIA

RELAZIONE PRELIMINARE N. 48 PER IL SIG. DIRETTORE E DETERMINAZIONE A CONTRARRE

ARGOMENTO: *Piano Nazionale della Ricerca Militare 2022 - Proposta n. a2021.144 dal titolo "ArIS - Artificial Intelligence Sandboxing". Fase 1 di 2.*

DATI IDENTITICATIVI ED IMPORTO PROGRAMMATO

Fascicolo: **22/04/056**	**CdG:** 035	**Capitolo:** 7101-1	**CPV:** 73100000-3	**Importo programmato (quota del 50% a carico dell'A.D):** **Fase 1 € 366.000,00 (IVA inclusa)** **Fase 2 € 347.700,00 (IVA inclusa) – opzionale.** **Codice A**

1. RIFERIMENTI:

a. Scheda di progetto PRNM n. a2021.144

b. Dp. Nr. M_D ABBE6E3 REG2022 0053754 del 26 luglio 2022 del V Reparto di SEGREDIFESA – Lettera di Mandato.

2. ESIGENZA DA SODDISFARE E PROFILO TECNICO

Il progetto di ricerca ArIS - Artificial Intelligence Sandboxing, presentato con la scheda in riferimento *a.*, è finalizzato alla realizzazione di una metodologia di test e validazione per i sistemi che facciano uso di sistemi di Intelligenza Artificiale. Il progetto mira all'elaborazione di metriche che permettano di valutare rapidamente ed efficacemente il livello di sicurezza di tecnologie che impieghino sistemi di intelligenza artificiale, permettendo di valutarne l'applicabilità anche in contesti critici (*mission critical*). Questo sarà realizzato individuando una metodologia per la quantificazione della robustezza dei sistemi nel loro complesso rispetto ad eventuali azioni di disturbo o inganno in ambiente operativo/applicativo.

Un secondo obiettivo del progetto è la creazione di un tool per il calcolo di questa metrica. Il concetto di sandbox, già in uso in altri ambiti della sicurezza cibernetica, offre a tal riguardo un ottimo sistema per assolvere questo compito: tramite questo progetto si vuole sviluppare un ambiente controllato di test in cui sottoporre i sistemi intelligenti a diverse metodologie di attacco restituendo all'utente un punteggio che permetta di interpretare facilmente il livello di robustezza raggiunto.

La scelta di una *sandbox* è in linea con la messa in atto del progetto delle *Regulatory Sandboxes* introdotta nella Strategia Italiana per l'Intelligenza Artificiale, in cui si suggerisce la definizione di un ambiente in cui testare nuovi prodotti, servizi, tecnologie.

3. RIFERIMENTI NORMATIVI PER LA SELEZIONE DEGLI OPERATORI ECONOMICI

La presente impresa rientra nell'ambito di applicazione del D. Lgs 15 novembre 2011, n. 208 e relativo regolamento applicativo di cui al D.P.R. 49/2013 e, per quanto in esso non espressamente previsto, si applicano le disposizioni del D.P.R. 236/2012 e, se del caso, del D.Lgs. 50/2016.

La procedura individuata per la selezione dell'operatore economico è la procedura negoziata senza pubblicazione di un bando ai sensi dell'art. 18 comma 3 lettera b) del D.Lgs. 208/2011 con la società Telsy

S.p.A., proponente del progetto in argomento denominato "ArIS", in quanto i prodotti oggetto del contratto saranno fabbricati esclusivamente a fini di ricerca e sviluppo.

Inoltre:

- il contraente è stato selezionato da SEGREDIFESA in esito alla conclusione della procedura prevista nel Regolamento interno per la "Ricerca Militare in campo Nazionale", SGD-G-024;
- l'argomento di ricerca è stato espressamente selezionato da SEGREDIFESA con l'obiettivo finale di realizzare una metodologia di test e validazione per i sistemi che facciano uso di sistemi di Intelligenza Artificiale;
- il contraente dispone della competenza scientifica e tecnica per sviluppare compiutamente l'attività di ricerca proposta.

Risultano inoltre assolti dall'attività preliminare di selezione del proponente, svolta da SGD in esito alla SGD-G-024, gli adempimenti di cui all'art.18 comma 7 del D.Lgs. 208/2011 in merito all'individuazione degli operatori economici da consultare.

4. PUBBLICITA' E TRASPARENZA

La pubblicazione dell'avviso di avvenuta aggiudicazione sarà effettuata sulla GUE e sul sito della Direzione. In relazione agli obblighi derivanti dal D.Lgs. 25 maggio 2016, n.97 ("Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza"), e in ottemperanza alle successive delibere ANAC volte a fornire le linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni, tutti gli atti saranno pubblicati in formato aperto ed editabile (p.e. utilizzando il formato PDF/A), prediligendo documenti in formato nativamente digitale e limitando al massimo, ed ai casi di effettiva necessità, l'allegazione di documenti analogici scansionati.

5. COMPENSAZIONI INDUSTRIALI

Non applicabile.

6. PRINCIPALI ELEMENTI CONTRATTUALI

a. Suddivisione in lotti

La fornitura per la fase 1 del progetto sarà articolata in 3 lotti.
Ogni Lotto sarà a sua volta articolato sui *Work Package* (WP) di seguito descritti:

Lotto 1: Analisi dello stato dell'arte
WP1 - Analisi dello stato dell'arte
WP1.1 - Analisi degli scenari di applicazione
WP1.2 - Analisi degli studi disponibili in letteratura
WP1.3 - Analisi di eventuali soluzioni industriali concorrenti
Lotto 2: Progettazione e sviluppo componente "core"
WP2: Progettazione e sviluppo componente "core"
WP2.1: Studio dei possibili attacchi e del loro impatto sugli scenari previsti
WP2.2: Progettazione delle metriche per misurare della robustezza dei sistemi di AI
Lotto 3: Scenario Image Classification/Recognition
WP3: Scenario Image Classification/Recognition
WP3.1: Studio e prima implementazione della soluzione nello scenario di Image Classification/Image Recognition
WP3.2: Analisi dei risultati e possibili generalizzazioni della metodologia applicata.

La fornitura per la fase 2 (opzionale) del progetto sarà articolata in 3 lotti.
Ogni Lotto sarà a sua volta articolato sui Work Package (WP) di seguito descritti:

Lotto 4: Image Classification/Recognition scenario - completamento sandbox.
WP4 - Image Classification/Recognition scenario - completamento sandbox.
WP4.1: Completamento e irrobustimento Sandbox.
WP4.2: Implementazione e test degli scenari di attacco.
Lotto 5: Scenario Malware analysis
WP5: Scenario Malware analysis
WP5.1: Progettazione e sviluppo del secondo scenario.
WP5.2: Implementazione supporto a una vasta gamma di attacchi di tipologie diverse.
Lotto 6: Ingegnerizzazione del progetto
WP6: Ingegnerizzazione del progetto
WP6.1: Ingegnerizzazione della sandbox per il supporto e l'analisi a diverse tipologie di prodotti e modelli di AI.
WP6.2: Test e validazione della qualità del codice.

b. Aggiudicazione per lotti separati
Non applicabile

c. Condizioni di pagamento:
Ai sensi dell'art. 4, comma 4 del D.Lgs. 9 ottobre 2002, n. 231 e dell'art. 113 bis del D.Lgs. 18 aprile 2016, n. 50, considerata la particolare natura del presente contratto, alla cui esecuzione devono partecipare diversi organi della Amministrazione della Difesa, aventi varia dislocazione nel territorio, i pagamenti saranno disposti entro 60 giorni decorrenti dalla data di emissione del Certificato di Pagamento; tale estensione del termine di pagamento sarà esplicitamente pattuita con la società contraente, oltre che sottoscritta nel successivo contratto.
Ai sensi dell'art. 35 comma 18 del D. Lgs 18 aprile 2016, n. 50, innovato dall' art. 207 comma 1 del D.L. 34/2020 i cui effetti sono stati prorogati con l'art. 3 comma 4 del D.L. n. 228/2021, viste le risorse garantite dall'organo programmatore con la lettera di mandato richiamata nei riferimenti, sarà prevista l'anticipazione del prezzo da corrispondere all'appaltatore entro quindici giorni dall'effettivo inizio della prestazione, subordinata alla costituzione di garanzia fideiussoria bancaria o assicurativa di importo pari all'anticipazione, maggiorato del tasso di interesse legale applicato al periodo necessario al recupero dell'anticipazione stessa secondo il cronoprogramma della prestazione. L'anticipazione del prezzo verrà scomputata dai pagamenti contrattualmente previsti.

Il pagamento per ciascun lotto sarà effettuato nel seguente modo:
- 100% dopo l'emissione del Certificato di pagamento.

d. Revisione prezzo
Sarà ammessa la revisione dei prezzi come previsto dall'art. 106 del D. Lgs 18 aprile 2016, n. 50 ai sensi dell'articolo 29 comma 1 lett. a) del DL 4/2022.

e. Garanzie per la partecipazione a gare e garanzia definitiva.
La garanzia definitiva ai sensi dell'art. 103 del D. Lgs 18 aprile 2016, n. 50, sarà pari al 10% del prezzo complessivo contrattuale ed è svincolato proporzionalmente all'esecuzione contrattuale.
Alla garanzia si applicano le riduzioni previste dall'art 93 comma 7 D. Lgs 18 aprile 2016, n. 50.

f. Assicurazione di qualità.
Non richiesta.

g. Subappalto
È ammesso il subappalto in conformità alla vigente normativa

h. Penalità:

In linea con le prescrizioni dell'articolo 125 del D.P.R. 236 del 2012, sarà prevista per ciascun lotto, una penalità pari allo 0,5 per mille del valore dello stesso per ogni giorno di ritardo. La penalità complessiva massima non potrà eccedere, comunque, il 10% dell'importo contrattuale.

7. RESPONSABILE UNICO O RESPONSABILE PER OGNI SINGOLA FASE DEL PROCEDIMENTO

Il Capo della 4ª Divisione pro-tempore, competente per materia, sarà il "Responsabile del Procedimento" ai sensi del D.lgs. 50/2016, art.31.

8. TEMPI DI ESECUZIONE CONTRATTUALE ED ELEMENTI FINANZIARI

a. Tempi di esecuzione

I tempi di esecuzione sono i seguenti.

FASE 1

- Lotto 1: 30 gg.ss. a decorrere dalla data di ricezione da parte del contraente della comunicazione di attivazione del Lotto 1;
- Lotto 2: 180 gg.ss. a decorrere dalla data di comunicazione da parte dell'A.D. dell'avvenuta verifica di conformità con esito positivo del Lotto 1
- Lotto 3: 150 gg.ss. a decorrere dalla data di comunicazione da parte dell'A.D. dell'avvenuta verifica di conformità con esito positivo del Lotto 2.

FASE 2 (opzionale)

- Lotto 4: 90 gg.ss. a decorrere dalla data di ricezione da parte del contraente della comunicazione di attivazione del Lotto 1;
- Lotto 5: 180 gg.ss. a decorrere dalla data di comunicazione da parte dell'A.D. dell'avvenuta verifica di conformità con esito positivo del Lotto 1
- Lotto 6: 90 gg.ss. a decorrere dalla data di comunicazione da parte dell'A.D. dell'avvenuta verifica di conformità con esito positivo del Lotto 2.

b. Profilo dell'impegno pluriennale ad esigibilità

Valutati i tempi per la contrattualizzazione, i tempi necessari per l'approvazione da parte degli Organi di Controllo ed i termini di esecuzione e collaudo delle singole attività oggetto di liquidazione del lotto (in calce tabella riepilogativa complessiva riportata nella lettera di mandato), si prevede, al meglio delle attuali conoscenze, il seguente profilo di impegno pluriennale ad esigibilità, allineato ai previsionali esiti di cassa. Detto profilo di impegno è allineato e coerente alle risorse garantite dall'Organo Programmatore con la lettera di mandato in riferimento e successive rimodulazioni approvate da SGD V Reparto.

All'atto dell'impegno di spesa, nel rispetto dell'art. 34 L. 196/2009, il profilo di impegno verrà attualizzato in relazione all'effettiva esigibilità. L'emissione del modello B di finanziamento, con le quote di competenza allineate all'effettiva esigibilità, darà evidenza della avvenuta rimodulazione delle quote di stanziamento inizialmente previste, da parte degli Organi Programmatori

FASE 1

COMPETENZA PROGRAMMATA (valori comprensivi di IVA)

2022	2023	2024	Tot. complessivo
€ 0	€ 256.200,00	€ 109.800,00	€ 366.000,00

CASSA PREVISIONALE (valori comprensivi di IVA)

2022	2023	2024	Tot. complessivo
0	€ 256.200,00	€ 109.800,00	€ 366.000,00

c. Programma degli acquisti

La presente impresa sarà riportata nel programma biennale degli acquisti ai sensi dell'art. 21 comma 7 del D.Lgs. 50/2016.

d. IVA
La fornitura è soggetta all'imposta sul valore aggiunto

e. Tracciabilità dei flussi finanziari
Sarà richiesto *SMART CIG* in quanto l'impresa rientra nell'ambito di applicazione del D.lgs 208/2011.

f. Variazione del patrimonio dello stato
Non ci sarà alcuna variazione del patrimonio dello stato in quanto si tratta di attività di ricerca che non prevede la fornitura di materiali all'A.D..

9. ULTERIORI ANNOTAZIONI

La regolamentazione della proprietà intellettuale e dei correlati diritti sarà trattata in accordo alle vigenti disposizioni applicative in materia.

Roma,

Il Capo della 4ª Divisione
C.V. (GN) Andrea PUGINA

Firmato Digitalmente da/Signed by:
ANDREA PUGINA
In Data/On Date:
lunedì 10 ottobre 2022 09:49:26

VISTO:
Il Capo del 2° Reparto f.f.
C.V. (GN) Giovanni TORRE

Firmato Digitalmente da/Signed by:
GIOVANNI TORRE
In Data/On Date:
lunedì 10 ottobre 2022 15:02:18

MINISTERO DELLA DIFESA

SEGRETARIATO GENERALE DELLA DIFESA E DIREZIONE NAZIONALE DEGLI ARMAMENTI

DIREZIONE DEGLI ARMAMENTI NAVALI

ARGOMENTO: *Piano Nazionale della Ricerca Militare 2022 - Proposta n. a2021.144 dal titolo "ArIS - Artificial Intelligence Sandboxing". Fase 1 di 2.*

Fascicolo: **22/04/056**	**CdG:** 035	**Capitolo:** 7101-1	**CPV:** 73100000-3	**Importo programmato (quota del 50% a carico dell'A.D):** **Fase 1 € 366.000,00 (IVA inclusa)** **Fase 2 € 347.700,00 (IVA inclusa) – opzionale.** **Codice A**

IL DIRETTORE

Visto
- quanto descritto nei punti da 1 a 9;

Considerata
- la necessità di procedere all'acquisizione di cui trattasi;

DECRETA

1. Che gli Uffici e le Divisioni interessati dal suddetto procedimento, ognuno per la parte di propria competenza, assicurino il soddisfacimento dell'esigenza prospettata e svolgano tutte le attività necessarie per addivenire alla stipulazione del contratto.

2. Che il C.V. Andrea PUGINA, in qualità di Capo della 4ª Divisione *pro tempore*, sia "Responsabile del Procedimento" ai sensi dell'art. 31 del D. Lgs 18 aprile 2016, nr. 50.

Roma,

IL DIRETTORE
Amm. Isp. Capo Massimo GUMA

Firmato Digitalmente da/Signed by:
MASSIMO GUMA
In Data/On Date:
lunedì 10 ottobre 2022 16:33:02