

COMANDO PER LE OPERAZIONI IN RETE

UFFICIO AMMINISTRAZIONE

Sezione Gestione Finanziaria e Contratti

C . F . 9 6 4 5 1 0 6 0 5 8 4

Via Stresa 31/B – 00135 ROMA

Posta elettronica: cor@cor.difesa.it

Posta elettronica certificata: cor@postacert.difesa.it

Lettera di Ordinazione n. 13

(da citare in fattura)

Roma, 10/03/2025

I & C INTERNATIONAL CONSULTING SRL
Largo Rodolfo Lanciani , 24 – ROMA
(PEC: IEC@PEC.INTCONSULTING.IT)

Oggetto: Gara 6 – Appalto al servizio di ingegneria per la progettazione omologazione, certificazione e mantenimento in corso di validità dei documenti Comsec per le esigenze del COR DIFESA. Cap. 7115/2 – CIG B584D93766 - CUP D87H25000030001. E.F. 2025. RDO 5043870.

IDV: 1924385

Rife: Obbligazione Commerciale nr. 1/2025 del 10/03/2025.

1. Codesta Ditta è risultata essere aggiudicataria della seguente fornitura, comprensiva dei relativi costi alla sicurezza, pari a euro **500,00** come da T.D. in oggetto:

Descrizione	imponibile
Appalto al servizio di ingegneria per la progettazione omologazione, certificazione e mantenimento in corso di validità dei documenti Comsec per le esigenze del COR DIFESA , come da R.T.O. in allegato.	€. 81.000,00
Totale imponibile	€. 81.000,00
IVA 22%	€. 17.820,00
TOTALE	€. 98.820,00

2. La presenta commessa, per tutto quanto non previsto nella presente, si svolgerà sotto l'osservanza del Codice dei contratti di cui al decreto legislativo 31 marzo 2023, nr. 36.
3. La Ditta si impegna ad eseguire la fornitura/prestazione a sua cura, rischio e spese **a decorrere dalla data di consegna/accettazione della presente e dovrà essere conclusa entro il giorno il 15/12/2025**, osservando tutte le norme e disposizioni indicate nella presente lettera di ordinazione
4. **Si precisa che la fattura elettronica dovrà essere obbligatoriamente emessa in data successiva all'ultimazione della fornitura/servizio** ovvero successivamente agli esiti positivi delle procedure previste ai fini dell'accertamento della conformità della fornitura/servizio (verbale di verifica conformità ove previsto) e comunque, **previa richiesta di autorizzazione al seguente indirizzo email: uam.sa.sca.cs@cor.difesa.it**; dovrà essere compilata in maniera analitica nelle modalità richieste, come sopra specificato, e dovrà indicare il numero di protocollo del presente ordinativo, il numero di CIG e CUP, la causale come da oggetto della presente lettera e l'annotazione "SCISSIONE DEI PAGAMENTI" (qualora in presenza di IVA da versare allo Stato). La stessa dovrà essere intestata ed inviata a: COMANDO PER LE OPERAZIONI IN RETE - Servizio Amministrativo - Via Stresa, n. 31/b – 00135 ROMA Codice Fiscale 96451060584. Codice Ufficio ai sensi dell'articolo 3, del Decreto MEF n. 55 del 3 aprile 2013 in materia di emissione, trasmissione e ricevimento della **fattura elettronica 2SR075**.
5. Il presente affidamento trova copertura finanziaria con risorse attestate sul **capitolo di bilancio 7115/2 dell'E.F. 2025** mediante apertura di credito a favore del Funzionario Delegato dell'Ufficio Generale Centro di Responsabilità Amministrativa (UGCRA).
6. La fornitura/prestazione dovrà essere effettuata a cura di codesta Ditta secondo le modalità riportate nell'Obbligazione Commerciale in riferimento.
7. **Direttore Esecuzione Contrattuale:** Magg. Domenico GIGANTI tel. 06/46914654 – mail: sed.usc.ssc.ad@cor.difesa.it

II CAPO SERVIZIO AMMINISTRATIVO
Col. com. Maurizio LAMBIASE
(documento firmato digitalmente)

FIRMA PER ACCETTAZIONE

IL RAPPRESENTANTE LEGALE DELLA DITTA

(documento firmato digitalmente)

COMANDO PER LE OPERAZIONI IN RETE



REQUISITO TECNICO-OPERATIVO

Acquisizione servizi di ingegneria a favore del COR

Edizione 2024

PREDISPOSIZIONE DEL DOCUMENTO

Redatto da	Data

QUESTO DOCUMENTO È COSTITUITO DA 12 PAGINE TOTALI

INDICE

1	INTRODUZIONE	4
1.1	IDENTIFICAZIONE E OGGETTO DEL DOCUMENTO	4
1.2	OGGETTO DEL CONTRATTO	4
1.3	DURATA DELL'APPALTO	4
2	DOCUMENTI, NORMATIVE E STANDARD DI RIFERIMENTO	5
2.1	NORMATIVE GENERALI	5
2.2	NORMATIVE INERENTI ALLA TUTELA DEL SEGRETO DI STATO	5
3	PRESCRIZIONI TECNICHE PARTICOLARI	7
3.1	INTRODUZIONE	7
3.2	PLANIMETRIE COMSEC/CIS	7
3.3	DOCUMENTI DI SICUREZZA	7
4	REQUISITI DI CAPACITÀ TECNICA E PROFESSIONALE	11
4.1	REQUISITI D'IDONEITÀ	11
4.2	ASSICURAZIONE DELLA QUALITÀ	11
4.3	SISTEMA DI SICUREZZA E SALUTE	11
4.4	SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI	11
4.5	SICUREZZA DELLE INFORMAZIONI	11

1 INTRODUZIONE

1.1 IDENTIFICAZIONE E OGGETTO DEL DOCUMENTO

Questo documento costituisce il requisito tecnico prestazionale relativo all'erogazione di servizi di *Information Assurance* necessari a supportare il Comando per le Operazioni in Rete, di seguito COR, per la progettazione, la certificazione/omologazione ed il mantenimento della certificazione/omologazione di prodotto, sistemi e infrastrutture classificate di sua competenza.

1.2 OGGETTO DEL CONTRATTO

L'esecuzione delle prestazioni previste nel presente requisito dovrà avvenire nel rispetto del Codice Civile e della deontologia professionale, svolgendo tutti gli adempimenti attribuiti allo specifico ruolo funzionale dalle leggi e dai regolamenti vigenti in materia di lavori pubblici.

La prestazione è composta da quelle attività ed elaborazioni, previste dalle normative vigenti in materia e ritenute necessarie per poter svolgere, con il grado di perfezione richiesto dal presente documento, le attività di:

- Redazione documenti di sicurezza necessari all'omologazione CIS per la rete VeVA (*Vigilance and Enhanced Vigilance Activity*¹) e al discendente adeguamento COMSEC del COR;
- Redazione planimetrie COMSEC/CIS necessarie al completamento della sopracitata documentazione.

1.3 DURATA DELL'APPALTO

Le attività richieste dovranno essere erogate nel corso del 2025 e concludersi nei tempi dettati dalle disposizioni normative vigenti.

¹ Per la descrizione della rete VeVA si rimanda a documentazione separata che il Comando per le Operazioni in Rete consegnerà esclusivamente alla ditta aggiudicataria.

2 DOCUMENTI, NORMATIVE E STANDARD DI RIFERIMENTO

2.1 NORMATIVE GENERALI

- [1] Decreto legislativo 31 marzo 2023, n. 36 Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici.
- [2] Decreto del Presidente della Repubblica 5 ottobre 2010 n. 207, "Regolamento di esecuzione ed attuazione del decreto legislativo 12 aprile 2006, n. 163, recante «Codice dei contratti pubblici relativi a lavori, servizi e forniture in attuazione delle direttive 2004/17/CE e 2004/18/CE.»" (Per quanto applicabile ai sensi dell'art. 217, lettera u) del D.Lgs. 18 aprile 2016, n. 50).
- [3] Decreto Legislativo 15 novembre 2011 n. 208, "Disciplina dei contratti pubblici relativi ai lavori, servizi e forniture nei settori della difesa e sicurezza, in attuazione della direttiva 2009/81/CE".
- [4] Decreto del Presidente della Repubblica 13 marzo 2013, n. 49, "Regolamento per la disciplina delle attività del Ministero della difesa in materia di lavori, servizi e forniture militari, a norma dell'articolo 4, comma 1, del decreto legislativo 15 novembre 2011, n. 208, recante attuazione della direttiva 2009/81/CE".
- [5] Decreto del Presidente della Repubblica 15 novembre 2012, n. 236 – "Regolamento concernente disciplina delle attività del Genio militare, a norma dell'articolo 196, del D.Lgs n. 163/06".
- [6] Decreto Legislativo 9 maggio 2001 n. 269, "Attuazione della direttiva 1999/5/CE riguardante le apparecchiature radio, le apparecchiature terminali di telecomunicazione e il reciproco riconoscimento della loro conformità".
- [7] Legge n. 186 del 3.1.1968 sull'esecuzione degli impianti elettrici.
- [8] Decreto nel Ministero per lo sviluppo economico 22 gennaio 2008 n. 37, "Regolamento concernente l'attuazione dell'articolo 11-quaterdecies, comma 13, lettera a) della legge n. 248 del 2005, recante riordino delle disposizioni in materia di attività di installazione degli impianti all'interno degli edifici".
- [9] Decreto Legislativo 9 aprile 2008 n. 81, "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro".
- [10] D.M. 17 giugno 2016 "Approvazione delle tabelle dei corrispettivi commisurati al livello qualitativo delle prestazioni di progettazione adottato ai sensi dell'articolo 24, comma 8, del decreto legislativo n. 50 del 2016".

2.2 NORMATIVE INERENTI ALLA TUTELA DEL SEGRETO DI STATO

- [11] Decreto del Presidente del Consiglio dei Ministri 6 novembre 2015 – "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva" (Decreto n. 5/2015) così come modificato dal regolamento adottato con DPCM 2 ottobre 2017, n. 3.
- [12] PCM-ANS/LG – VAL, Linea Guida "Procedure di Valutazione" Versione 1.0, 18/03/2005.

- [13] PCM-ANS/LG – PP ST, Linee Guida per la realizzazione dei piani di valutazione cui devono attenersi il personale dei CE.VA., il Committente e il Fornitore dei sistemi e dei prodotti destinati alla trattazione delle informazioni classificate “Guida alla scrittura dei *Protection Profile* e dei *Security Target*”, Versione 1.0, 25/10/2002.
- [14] PCM-ANS/TI-001-005 e 008, Direttive tecniche in materia di sicurezza di sistemi e prodotti informatici.
- [15] Direttiva PCM-ONS 1/2019, “Disposizioni applicative del DPCM n. 5/2015 in materia di rilascio di abilitazioni di sicurezza per le PERSONE FISICHE”.
- [16] Direttiva PCM-ONS 2/2019, “Disposizioni applicative del DPCM n. 5/2015 in materia di rilascio di abilitazioni di sicurezza per gli OPERATORI ECONOMICI”.
- [17] Direttiva PCM-ONS 3/2019, “Disposizioni applicative del DPCM n. 5/2015 per la protezione delle informazioni classificate, a diffusione esclusiva, o coperte da segreto di Stato trattate con sistemi informatici e sistemi di comunicazione elettronici”.
- [18] Direttiva PCM-ANS 6/2006, “Misure di sicurezza materiale per la salvaguardia delle informazioni classificate”.
- [19] D.P.C.M. 11 aprile 2002 “Schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato”.
- [20] PCM-ANS/COMSEC-256 (B), “Installazione d'apparati elettrici per l'elaborazione di informazioni classificate”.
- [21] NATO C-M(2002)49-COR12, “*Security within the North Atlantic Treaty Organisation*”, *Corrigendum to C-M(2002)49 dated 17 June 2002 Amendment 12*.
- [22] NATO SDIP-29/2, “*Facility design criteria and installation of equipment for processing of classified information*”.
- [23] NATO SDIP-28/2, “*NATO Zoning Procedure*”.
- [24] NATO SDIP-27/2 Level A, “*Compromising emanations laboratory test standard*”.
- [25] NATO SDIP-27/2 Level B, “*Compromising emanations laboratory test standard*”.
- [26] NATO SDIP-27/2 Level C, “*Laboratory test standard for tactical mobile equipment/system*”.
- [27] 2013/488/EU, “*Council Decision of 23 Sep 2013 on the security rules for protecting EU classified information*”.
- [28] 2015/444, “*Commission Decision of 13 March 2015 on the security rules for protecting EU classified information*”.
- [29] IASP 7, “*Information Assurance Security Policy on TEMPEST*”.
- [30] IASG 7-01, “*IA Security Guidelines on Selection and Installation of TEMPEST Equipment*”.
- [31] IASG 7-02, “*IA Security Guidelines on TEMPEST Zoning Procedures*”.
- [32] IASG 7-03, “*IA Security Guidelines on EU TEMPEST Requirements and Evaluation Procedures*”.

3 PRESCRIZIONI TECNICHE PARTICOLARI

3.1 INTRODUZIONE

La presente sezione descrive le caratteristiche peculiari a cui dovranno rispondere le prestazioni e i servizi previsti dal requisito.

3.2 PLANIMETRIE COMSEC/CIS

Al fine di ottemperare a quanto richiesto dalle procedure nazionali necessarie all'omologazione di sistemi che trattano informazioni classificate, devono essere redatte in conformità alla direttiva PCM-ANS-256B le Planimetrie COMSEC/CIS. Le planimetrie dovranno essere consegnate al COR per la necessaria approvazione. Per la redazione delle stesse si dovranno rispettare le seguenti disposizioni: in generale, per ogni locale classificato e comunque ogni locale interessato dalla realizzazione di sistemi classificati, come prescritto dalla normativa, dovrà essere prodotta la rappresentazione in pianta e i quattro prospetti delle pareti.

Ciascuna tavola dovrà riportare in evidenza:

- Identificazione (tipo e sigla) e posizione degli apparati classificati previsti.
- Identificazione e posizione dei filtri di alimentazione e segnale.
- Identificazione e posizione degli apparati telefonici.
- Identificazione e posizione altri apparati come apparecchiature terminali appartenenti ad altri sistemi.
- Identificazione e posizione dei contenitori di sicurezza.
- Identificazione e posizione dei dispositivi dell'impianto antintrusione.
- Identificazione e posizione delle attrezzature per la distruzione materiale classificato.
- Identificazione e posizione dei corpi illuminanti.
- Percorso e tipo dei conduttori fortuiti.
- Percorso e tipo dei cavi elettrici, segnale e fibre ottiche NERE.
- Percorso e tipo dei cavi elettrici, segnale e fibre ottiche ROSSE.
- Posizione e tipo apparati nei locali adiacenti, sopra e sotto che non rispettano le distanze minime previste.

3.3 DOCUMENTI DI SICUREZZA

Al fine di ottenere l'omologazione degli ambienti classificati, il Comando per le Operazioni in Rete necessita di produrre apposita documentazione di sicurezza in accordo alla Direttiva [17].

In relazione alla tipologia di sistema, prodotto o infrastruttura da far approvare, le caratteristiche della documentazione da redigere sono riportate qui di seguito.

- Requisiti Specifici di Sicurezza del Sistema: che descrivono i requisiti di sicurezza a cui deve rispondere il CIS per la protezione delle informazioni classificate in esso trattate. Il docu-

mento RSSS dovrà contenere, tra l'altro, i seguenti punti e comunque prevedere le informazioni richiamate in allegato 3 del PCM-ONS 3 del 2019:

- “Generalità”: descrizione della tipologia di CIS che si intende realizzare. In questo paragrafo sono riportati, tra l'altro, il massimo livello di classifica e qualifica delle informazioni classificate trattate, il numero e la tipologia di utenti autorizzati all'impiego del CIS, gli obiettivi e le funzioni di sicurezza del sistema informatico;
 - “Descrizione e rappresentazione grafica del CIS”: descrizione dell'architettura e della configurazione hardware e software del CIS e dei relativi collegamenti fisici e funzionali;
 - “Compiti e responsabilità dell'organizzazione di sicurezza CIS”: compiti e responsabilità dell'organizzazione di sicurezza e degli utenti;
 - “Ambienti di sicurezza”: delimitazione e descrizione dell'Ambiente di sicurezza globale (ASG), dell'Ambiente di sicurezza locale (ASL) e dell'Ambiente di sicurezza elettronico (ASE) come definiti al precedente paragrafo 4.2.2;
 - “Requisiti di sicurezza del CIS”: descrizione dettagliata dei requisiti di sicurezza fisica, tecnica, personale e procedurale da soddisfare per la protezione delle informazioni classificate trattate dal CIS. Nel caso di CIS distribuiti in rete geografica, sono descritti i requisiti operativi e di sicurezza delle interconnessioni;
 - “Misure di sicurezza del CIS”: descrizione delle misure di sicurezza da predisporre per la protezione del CIS.
- Analisi del Rischio che ha l'obiettivo, mediante l'identificazione e la valutazione delle minacce e delle vulnerabilità cui i sistemi per la gestione, l'elaborazione e la comunicazione delle informazioni classificate sono soggetti, di definire le misure di sicurezza da adottare per la protezione del patrimonio informativo classificato, riducendo il rischio di violazioni e di compromissioni di sicurezza ad un livello accettabile. L'Analisi del rischio dovrà essere elaborata prendendo a riferimento gli standard e le migliori pratiche applicabili e dovrà contenere i seguenti punti:
- Individuazione del patrimonio fisico e informativo gestito e del correlato perimetro di applicazione di eventuali misure di protezione;
 - Individuazione e classificazione delle singole minacce e delle possibili “modalità di attacco” mediante le quali ciascuna minaccia potrebbe attuarsi;
 - Individuazione e classificazione delle vulnerabilità che possono essere sfruttate con successo in relazione alle minacce individuate;
 - Valutazione del rischio in assenza di adozione di contromisure;
 - Individuazione e classificazione delle contromisure applicabili per la mitigazione del rischio;
 - Valutazione del rischio residuo;
 - Accettazione del rischio residuo.
- Regolamento di sicurezza CIS che descrive le misure di sicurezza adottate e le procedure da seguire per il soddisfacimento dei requisiti di sicurezza fisica, personale, procedurale e tecnica definiti nel documento RSSS. Lo schema del Regolamento Interno di sicurezza è riportato in Allegato 4 del PCM-ONS 3 del 2019 e dovrà contenere i seguenti punti:
- “Introduzione”: descrizione del CIS, tipologia, massimo livello di classifica delle informazioni classificate elaborate e memorizzate, relative modalità operative;

- “Responsabilità e compiti”: descrizione delle responsabilità e dei compiti del personale operante nell’organizzazione di sicurezza CIS e dei relativi utenti;
 - “Sicurezza fisica”: descrizione generale dell’infrastruttura (in relazione alla suddivisione in ASG, ASL ed ASE come definiti al precedente paragrafo 4.2.2) e dell’area riservata o controllata in cui è installato il CIS, evidenziando le protezioni attive e passive adottate e le modalità di controllo dell’accesso al CIS da parte del personale autorizzato al relativo impiego;
 - “Sicurezza personale”: descrizione delle modalità con le quali l’organizzazione di sicurezza verifica il possesso, da parte del personale che utilizza il CIS, della necessità di conoscere e delle prescritte abilitazioni di sicurezza e delle modalità di istruzione del personale autorizzato all’impiego del CIS;
 - “Gestione in sicurezza dei supporti CIS e delle stampe prodotte”: modalità di gestione dei supporti CIS (etichettatura, contabilizzazione, consultazione e distruzione) e delle stampe prodotte (log delle stampe);
 - “Sicurezza tecnica dell’installazione e soluzioni TEMPEST”: descrizione delle modalità di installazione del CIS e delle misure adottate per il soddisfacimento dei requisiti TEMPEST;
 - “Sicurezza tecnica delle comunicazioni (COMSEC)”: descrizione, in caso di CIS distribuiti in rete geografica, delle installazioni COMSEC per realizzare i collegamenti geografici;
 - “Sicurezza hardware”: descrizione della configurazione hardware (completa di numeri seriali dei singoli dispositivi) da installare e delle procedure per il mantenimento della configurazione hardware approvata;
 - “Sicurezza software”: descrizione della configurazione software da installare (quali, tra l’altro, il sistema operativo, applicazioni *antimalware*, applicazioni per l’office automation) e delle procedure per la relativa installazione ed aggiornamento;
 - “Terminali remoti e requisiti di interconnessione”: descrizione, in caso di CIS distribuiti in rete geografica, dei nodi terminali e delle modalità di soddisfacimento dei requisiti di sicurezza di interconnessione tra i componenti del CIS, riportati nel documento RSSS;
 - “Monitoraggio e audit”: descrizione delle procedure per il monitoraggio delle informazioni e degli eventi relativi agli aspetti di sicurezza del sistema e per la verifica della conformità e dell’efficienza del CIS. Tale paragrafo descrive inoltre le responsabilità degli operatori che effettuano le operazioni di audit e la programmazione delle attività di audit;
 - “Continuità operativa e procedure di emergenza”: identificazione delle soluzioni e delle procedure in grado di garantire la continuità operativa del CIS e la gestione di incidenti, disastri naturali o interruzioni intenzionali o accidentali dei servizi erogati dal CIS;
 - “Controllo di configurazione e ciclo di vita del CIS”: procedure per l’identificazione, il controllo, la contabilizzazione, la distribuzione, la verifica e la dismissione dei componenti hardware e software durante l’intero ciclo di vita del CIS.
- Regolamento di sicurezza COMSEC che descrive le procedure operative e le misure di sicurezza adottate a soddisfacimento dei requisiti definiti nella relativa documentazione di progetto, il cui schema è riportato all’Allegato 12 del PCM-ONS 3 del 2019 e dovrà contenere i seguenti punti come già riportato per il Regolamento di sicurezza CIS:
- Introduzione;

- Responsabilità e compiti dell'organizzazione COMSEC;
- Sicurezza fisica;
- Sicurezza del personale;
- Sicurezza tecnica dell'installazione e soluzioni TEMPEST;
- Sicurezza tecnica delle comunicazioni (COMSEC);
- Sicurezza del materiale COMSEC;
- Procedure di emergenza;
- Controllo di configurazione e ciclo di vita degli apparati COMSEC e delle soluzioni di schermatura del centro;
- Eventuali allegati.

4 REQUISITI DI CAPACITÀ TECNICA E PROFESSIONALE

Le prestazioni dovranno essere espletate e fornite nel rispetto delle modalità disciplinate dalle normative e direttive elencate alla sezione 2.

4.1 REQUISITI D'IDONEITÀ

L'Operatore Economico dovrà essere iscritto nel registro delle imprese tenuto dalla Camera di commercio industria, artigianato e agricoltura per attività coerenti con quelle oggetto del presente capitolato (assimilabili a servizi d'ingegneria).

Ai sensi dell'art. 46 del Codice dei Contratti Pubblici e del Decreto del Ministero delle Infrastrutture 2 dicembre 2016, n. 263, i professionisti che espletano l'incarico di produzione dei documenti di sicurezza dovranno essere in possesso di laurea in ingegneria o in una disciplina tecnica attinente all'attività oggetto del presente documento, oppure aver ottenuto certificazioni tecniche su tematiche inerenti alle attività oggetto del presente capitolato.

Il personale incaricato dell'Operatore Economico della gestione ed erogazione delle varie prestazioni specialistiche dovrà avere esperienza nell'iter di certificazione/omologazione di sistemi e prodotti classificati secondo il DPCM 11/04/2002.

4.2 ASSICURAZIONE DELLA QUALITÀ

L'Operatore Economico dovrà eseguire l'attività nell'ambito di un sistema di qualità secondo le norme UNI EN ISO 9001:2015 certificato nel settore EA 33.

4.3 SISTEMA DI SICUREZZA E SALUTE

L'Operatore Economico dovrà essere dotato di un sistema di gestione della sicurezza e salute sul lavoro secondo le norme ISO 45001:2018 certificato.

4.4 SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

L'Operatore Economico dovrà essere dotato di un sistema di gestione della sicurezza delle informazioni secondo lo standard UNI CEI EN ISO/IEC 27001:2017 per la documentazione tecnica ed i servizi per la valutazione della sicurezza di sistemi e prodotti ICT.

4.5 SICUREZZA DELLE INFORMAZIONI

L'affidamento prevede attività che implicano l'accesso a informazioni classificate. In tal senso, in ottemperanza a quanto disposto dall'art. 44 del DPCM 6 novembre 2015, n. 5 così come modificato dal regolamento adottato con DPCM 2 ottobre 2017, n. 3, l'Operatore Economico dovrà essere in possesso di NOSI a livello SEGRETO/NATO SECRET in corso di validità e il personale impiegato per le lavorazioni dovrà avere il NOS in corso di validità almeno a livello SEGRETO/NATO SECRET.

Per lo svolgimento dell'incarico, l'Operatore Economico dovrà utilizzare un complesso di apparati, aree ad accesso riservato, personale abilitato, *hardware*, *software* e procedure operative, finalizzato all'elaborazione, memorizzazione e trasmissione di informazioni classificate o coperte da segreto di Stato, attraverso sistemi informatici; pertanto, l'Operatore Economico dovrà essere in possesso di un CIS approvato e omologato dall'UCSe per la trattazione di informazioni classificate o coperte da segreto di Stato fino al livello di SEGRETO/NATO.

In generale, la lista delle classifiche delle informazioni trattate nello svolgimento delle attività è riportata qui di seguito.

LISTA DELLE CLASSIFICHE DI SEGRETEZZA					
PER LA FORNITURA DI: "SERVIZI DI <i>INFORMATION ASSURANCE</i> A SUPPORTO DEL COR".					
DOCUMENTI E PARTI		S	RR	R	Non Class.
GENERICI					
0.1	Lettera di Ordinazione				X
0.2	Esistenza del contratto				X
0.3	Ordini di servizio, verbali amministrativi e certificati di collaudo			X	X
DOCUMENTI E ATTIVITÀ RESE DALL'IMPRESA AFFIDATARIA					
1.1	Planimetrie COMSEC/CIS		X	X	
1.2	Documentazione di sicurezza		X	X	X
1.3	Accesso a siti	X	X	X	X

Di seguito il dettaglio di previsione annuale:

Descrizione	Previsione costi 2025	Previsione costi 2026	Previsione costi 2027	Costo complessivo
Acquisizione servizi di ingegneria a favore del COR.	100.000,00 €	100.000,00 €	100.000,00 €	300.000,00€

Ai fini della validità dell'offerta, la stessa va presentata seguendo lo schema seguente.

Per informazioni a carattere amministrativo-procedurale:

SCHEMA DI OFFERTA

Allo **COMANDO OPERAZIONI IN RETE**
Ufficio Amministrazione - Sezione Gestione
Finanziaria e Contratti
Via Stresa, 31/B

Oggetto: Gara 6 – Appalto al servizio di ingegneria per la progettazione omologazione, certificazione e mantenimento in corso di validità dei documenti Comsec per le esigenze del COR DIFESA - Importo massimo previsto €. 81.967,00 (ottantunomilanovecentosessantasette/00) iva 22% esclusa.

Il sottoscritto LIDIA RAICOVICH RAINIERI nella sua qualità di AMMINISTRATORE UNICO della Ditta I&C INTERNATIONAL CONSULTING SRL, pec IEC@PEC.INTCONSULTING.IT residente in ROMA Via VINCENZO ARANGIO RUIZ 19, Codice fiscale/partita I.V.A. n. 05035031003 presenta la seguente offerta:

TIPOLOGIA	Qtà richieste	Prezzo unitario	TOTALE COMPRENSIVO COSTI SICUREZZA, come da offerta MEPA (A)
Appalto al servizio di ingegneria per la progettazione omologazione, certificazione e mantenimento in corso di validità dei documenti Comsec per le esigenze del COR DIFESA, come da R.T.O. in allegato.		€ 0,00	€ 81.000,00
N.B. ALLEGARE DETTAGLIO ANALITICO PREZZI OFFERTI SUDDIVISO PER COSTO UNITARIO DEI MATERIALI E/O ATTIVITA' DA SVOLGERE COME DA REQUISITI TECNICI IN ALLEGATO		ONERI DELLA SICUREZZA (a cura stazione appaltante qualora previsti non soggetti a ribasso) (B)	€ 0,00
		COSTI SICUREZZA a cura Ditta indicazione obbligatoria (solo da indicare) *	€ 500,00
		INDICAZIONE DEI COSTI PER LA MANODOPERA FACENTI PARTE DELL'IMPORTO OFFERTO NEL PRESENTE SCHEMA (se lavori o servizi)	€ 0,00
		IMPORTO IMPONIBILE	€ 81.000,00
		IVA 22%	€ 17.820,00
		Totale Offerta	€ 98.820,00

* Ai sensi dell'art. 26, comma 6, del D.Lgs. 9 aprile 2008, n.81 e del D.L. n. 70/2011 "Decreto sviluppo", è obbligatoria l'indicazione dei costi per la sicurezza.

La presente offerta ha validità fino al 31/12/2025.

L'OFFERENTE

timbro e firma