Anexa la AP 9541/11.01.2023

Finanțat de Uniunea Europeană NextGenerationEU

Planul Național de Redresare și Reziliență

Secțiunea III

CAIET DE SARCINI

Laborator cybersecurity-cyberdefence (CyberLab)

1. Introducere

Caietul de sarcini face parte integrantă din documentația de atribuire și constituie ansamblul cerințelor pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică.

Caietul de sarcini conține, în mod obligatoriu, specificații tehnice. Acestea definesc, după caz și fără a se limita la cele ce urmează, caracteristici referitoare la nivelul calitativ, tehnic și de performanță, siguranța în exploatare, dimensiuni, precum și sisteme de asigurare a calității, terminologie, simboluri, teste și metode de testare, ambalare, etichetare, marcare, condițiile pentru certificarea conformității cu standarde relevante sau altele asemenea. Caietul de sarcini trebuie să precizeze și instituțiile competente de la care furnizorii, executanții sau prestatorii pot obține informații privind reglementările obligatorii referitoare la protecția muncii, la prevenirea și stingerea incendiilor și la protecția mediului, care trebuie respectate pe parcursul îndeplinirii contractului și care sunt în vigoare la nivel național sau, în mod special, în regiunea ori în localitatea în care se execută lucrările sau se prestează serviciile ori operațiunile de instalare, accesorii furnizării produselor (după caz). În cadrul acestei proceduri, U.M. 02192 Constanța - Academia Navală „Mircea cel Bătrân" îndeplinește rolul de Autoritate contractantă.

Pentru scopul prezentei secțiuni a Documentației de Atribuire, orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

2. Contextul realizării acestei achiziții de produse

2.1. Informații despre Autoritatea contractantă

U.M. 02192 Constanța - Academia Navală „Mircea cel Bătrân" este o instituție publică de educație și cercetare științifică, ce oferă programe acreditate de licență și masterat pentru studii universitare în domeniul maritim, fluvial și portuar. Misiunea este formarea la nivel universitar a absolvenților care să satisfacă nevoia de profesioniști a Forțelor Navale Române și mediului economic din domeniul naval și portuar maritim și fluvial.

2.2. Informații despre contextul care a determinat achiziționarea produselor

Academia Navală „Mircea cel Bătrân" (ANMB), este o instituție publică de educație și cercetare științifică etalon a învățământului românesc de marină, cu 150 de ani de tradiție. ANMB oferă programe acreditate de licență și masterat pentru studii universitare în domeniul Inginerie Marina și Navigație, cu specializări multiple, dintre care enumerăm Navigație, hidrografie și echipamente navale – NHEN (secția militară), Electromecanica Navala – EN (secțiile militară si civilă) și Sisteme Electromecanice Navale – (secția civilă).

Securitatea cibernetică, în special in domeniul maritim, trebuie să abordeze probleme extrem de dificile, deoarece industria maritimă reprezintă o zona de intersecție a infrastructurilor critice (inginerie economică, tehnologii și sisteme de telecomunicații, ingineria și protecția mediului în industrie, energetică), în care riscul de contagiune si al efectelor conexe, greu de estimat, este unul foarte mare.

În cadrul disciplinelor predate la programe de studii vizate, în vederea dobândirii competențelor specifice de care viitorii absolvenți vor avea nevoie, cursanții vor explora cele mai bune practici și tehnici de securitate cibernetică, de ultimă oră, tehnici care îi vor ajuta să protejeze infrastructura IT și datele critice de atacurile cibernetice, dar și sistemele vitale întâlnite astăzi la bordul navelor militare și civile. Gravitatea acestor posibile atacuri ar putea perturba securitatea națională regională sau europeană, mediul de afaceri (atât pe mare,

cât și pe țărm), provocând pierderi financiare grele și, în cel mai rău caz, provocând pierderi de vieți omenești și dezastre majore de mediu.

Datorită naturii sale internaționale, sectorul maritim este un obiectiv din ce în ce mai atractiv pentru criminalitatea informatică, amenințările cibernetice maritime nefiind încă suficient de bine înțelese sau luate în serios. Totodată, dacă ținem cont de faptul că domeniul maritim înglobează astăzi o rețea vastă de companii de transport maritim, companii de asigurări, operatori offshore și onshore, operatori portuari; autorități naționale și internaționale, militari și părți interesate; nave și platforme maritime; încărcături, containere și infrastructură portuară; navigație, management maritim, sisteme de comunicații prin satelit, etc., realizăm magnitudinea acestui tot unitar care trebuie să conlucreze pentru a preveni atacurile cibernetice maritime și pentru a gestiona impactul atacurilor atunci când acestea apar.

În cadrul Academiei Navale „Mircea cel Bătrân", studenții desfășoară activități teoretice și practice în cadrul orelor de curs și laborator (pe platforme externe freeware), unde conștientizează și se familiarizează cu domeniul Cyber (Cybersecurity – Cyberdefence – Cyberterorism). În prezent, instituția nu deține un laborator propriu (Cyber), dedicat desfășurării instruirii studenților/masteranzilor în conștientizarea, prevenirea, identificarea, clasificarea și contracararea posibilelor atacuri cibernetice din domeniul maritim.

Misiunea Academiei Navale este de a forma la nivel universitar absolvenți care să satisfacă nevoia de profesioniști a Forțelor Navale Române și a mediului economic din domeniul ingineriei marine, naval și portuar maritim și fluvial. Astfel, prin constituirea unui Laborator Cyber în Academia Navală "Mircea cel Bătrân" se poate realiza pregătirea profesională la un nivel superior a echipajelor navelor militare/civile, implicit a studenților și masteranzilor, militari și civili, în conformitate cu standardele europene și cu necesitățile de antrenament ale echipajelor militare/civile în scenarii specifice, într-un regim economic din punct de vedere al resurselor consumate, cu scopul însușirii cunoștințelor și experienței necesare de către personalul militar/civil.

Existența unui Laborator cybersecurity-cyberdefence (CyberLab) permite păstrarea nivelului de acuratețe și de actualitate a serviciilor de educație livrate de către Academia Navală beneficiarilor săi și îmbunătățește experiența de învățare pentru studenți/masteranzi. Astfel, Academia Navală "Mircea cel Bătrân" poate dovedi atât comisiilor de evaluare instituțională periodice ale ARACIS, cât și comisiilor de monitorizare anuale ale Autorității Navale Române, că baza materială de care dispune este una de calitate, pentru a oferi cursanților și beneficiarilor săi un act didactic și de instruire la cele mai înalte standarde.

Necesitatea achiziției rezidă din două aspecte:

- nevoia tot mai crescută de specialiști foarte bine pregătiți care să asigure viitorul navigației și al infrastructurii conexe, bazată pe un grad ridicat de automatizare si securitate, cu nave autonome programate din ce in ce mai multe care să satisfacă totodată paradigma securității cibernetice;
- creșterea durabilă, axată pe rolul sporit al securității infrastructurii IT si IA de la bordul navelor moderne, implicit pe securitatea și reziliența cibernetică.

3. Descrierea produselor solicitate

3.1. Descrierea situației actuale la nivelul Autorității contractante

La data întocmirii prezentei documentații, U.M. 02192 Constanța - Academia Navală „Mircea cel Bătrân" nu deține un Laborator Cyber propriu, dedicat desfășurării instruirii studenților în conștientizarea, prevenirea, identificarea, clasificarea, contracararea posibilelor atacuri cibernetice, prin oferirea de soluții viabile rapide și, totodată, să ofere un mediu colaborativ si competitiv de antrenare, testare și diseminare a informațiilor, urmare a competițiilor locale, naționale sau internaționale, purtate între diverse echipe.

Laboratorul este necesar Autorității contractante pentru dezvoltarea bazei materiale, asigurând pregătirea profesională la un nivel superior a echipajelor navelor militare, cât și a studenților / masteranzilor, militari și civili, în conformitate cu standardele europene.

3.2. Obiectivul general la care contribuie furnizarea produselor

Achiziționarea produselor în termenele stabilite prin documentația de atribuire are un rol determinant pentru buna desfășurare a activităților Academiei Navale „Mircea cel Bătrân" stabilite în Planul cu Principalele Activități.

3.3. Produsele solicitate și operațiunile cu titlu accesoriu necesare a fi realizate

3.3.1 Produsele solicitate

DENUMIRE PRODUSE– Laborator cybersecurity-cyberdefence (CyberLab)

Nr. crt.	Denumire produs	Cantitate	Unitate de măsură	Loc de livrare	Specificații tehnice / cerințe funcționale	Durata minima garanție/termen de valabilitate
1	**Laborator cybersecurity-cyberdefence (CyberLab)**	**1**	**Cpl**	**- la sediul autorității contractante (str. Fulgerului nr.1, Constanța)**	***conform specificațiilor tehnice***	• perioada de garanție acordată produselor: ***minim 24 luni.*** • perioada de mentenanță: ***minim 36 luni.***

Componente

Nr. crt.	Denumire componentă	Unitate de măsură	Cantitate
1.	**Laborator cybersecurity-cyberdefence (CyberLab)**	**complet**	**1**
1.1	**Hardware CyberLab** **1 x SERVER cu toate cablările necesare**	**complet**	**1**
1.1.1	Procesor (minim 64Coruri/procesor)	bucată	2
1.1.2.	Memorie RAM (minim 1TB)	bucată	1
1.1.3	1.92TB SSD vSAS Read Intensive 12Gbps 512e 2.5in w/3.5in HYB CARR ,AG Drive SED, 1DWPD,	bucată	6
1.1.4	16TB HDD SAS 12Gbps 7.2K 512e 3.5in Hot-Plug	bucată	2
1.1.5	Ethernet 10/25G LAN	bucată	2
1.1.6	Sina glisanta pentru rackuri, cu suport pentru brațul de gestionare a cablurilor	bucată	1
1.2	**Software CyberLab**	**complet**	**1**
1.2.1	Licență acces Cybersecurity CLOUD Apps (3 ani)	bucată	1
1.2.2.	Open Source Cloud Computing Infrastructure	bucată	1
1.2.3.	Open source relational database	bucată	1
1.3.	**Training instructori ANMB**	**complet**	**1**
1.4.	**Suport tehnic si mentenanță (3 ani)**	**complet**	**1**

Specificații tehnice:

A. Specificații tehnice generale

Laboratorul Cyber va trebui să asigure instruirea studenților / masteranzilor la un nivel superior.

1.	Cerințe generale
1.1.	Toate echipamentele furnizate trebuie să fie noi (nu pot fi refurbished).
1.2.	Furnizorul (Contractantul) trebuie să se asigure că producătorul nu a anunțat sfârșitul duratei de viață sau întreruperea echipamentelor sau a software-ului.
1.3.	Furnizorul (Contractantul) trebuie să se asigure că nu este instalat niciun software suplimentar în echipamentul livrat, care nu este necesar pentru funcționalitatea

	echipamentului și a Laboratorului Cyber.
2.	**Cerințe generale pentru asamblarea și instalarea echipamentelor propuse**
2.1.	Toate echipamentele trebuie livrate în ambalajul original al producătorului și asamblate în spațiile specificate de cumpărător în România respectiv la sediul ANMB.
2.2.	Hardware-ul utilizat pentru Laboratorul Cyber trebuie să fie multi-rol. Atunci când este necesar, serverele pot fi readaptate la alte sarcini sau dezasamblate.
2.3.	Conectarea echipamentelor – toate echipamentele propuse trebuie să fie conectate la rețeaua de energie electrică. Trebuie să se efectueze operațiile (cablarea, marcarea și etichetarea) necesare, iar documentația tehnică trebuie să fie pregătită;
2.4.	Testarea echipamentelor – după instalarea echipamentul și implicit a software-ului laboratorului, contractantul, împreună cu reprezentanții cumpărătorului, trebuie să efectueze testarea echipamentelor în conformitate cu scenariile de testare convenite în prealabil și să ofere rezultatele testării în format hârtie și electronic.

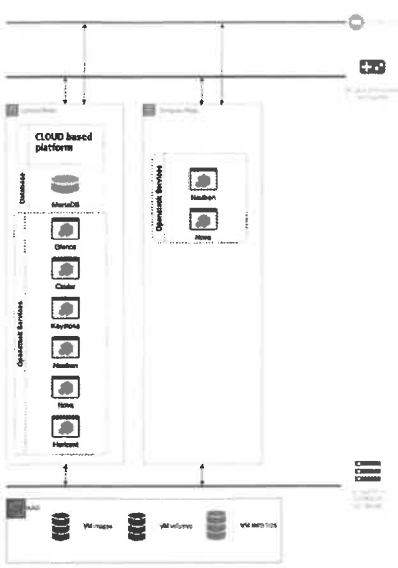
Cerințe tehnice minimale:

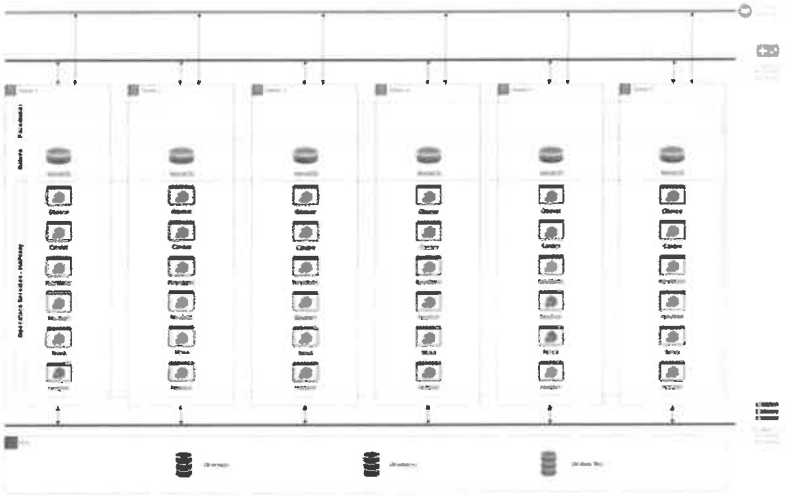
- Serverul trebuie să ofere suficientă putere de calcul pentru a furniza până la 300 de mașini virtuale utilizatorilor platformei;
- Software-ul se referă numai la operabilitatea platformei, prin urmare, nu include toate produsele software incluse în instruirea furnizată cu biblioteca de instruire a platformei.
- Platforma trebuie să fie complet independentă de licențiere și nelimitată în utilizare (nu trebuie să necesite licențe suplimentare pentru virtualizare.);
- Platforma trebuie să fie scalabilă prin adăugarea de componente hardware fără alte licențe suplimentare decât licențele cerute de Microsoft.
- Platforma trebuie să aibă la bază un sistem de lucru bazat pe CLOUD care să permită controlul unei game largi de resurse de calcul, stocare și rețea în cadrul unui centru de date. Infrastructura Open Source Cloud Computing trebuie să fie împărțită în servicii pentru a permite conectarea și lucrul cu componente ale bibliotecii de exerciții, în funcție de nevoi.

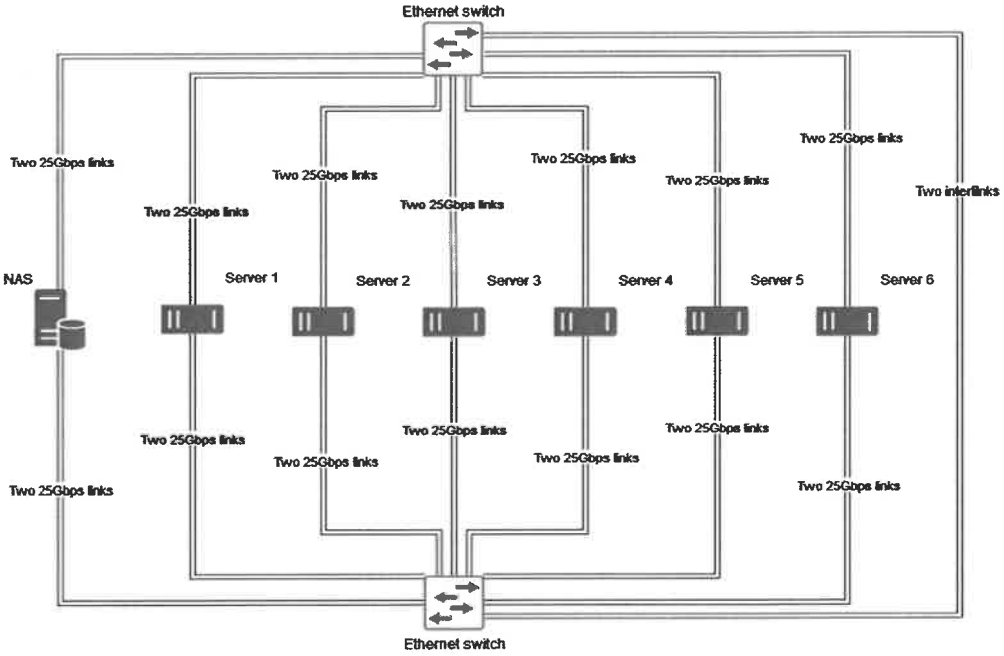
B. Specificații tehnice detaliate

I. Laborator cybersecurity-cyberdefence (CyberLab)

Laboratorul Cyber va permite instruirea studenților/masteranzilor în conștientizarea, prevenirea, identificarea, clasificarea, contracararea posibilelor atacuri cibernetice, prin oferirea de soluții viabile rapide și, totodată, să ofere un mediu colaborativ si competitiv de antrenare, testare și diseminare a informațiilor, urmare a competițiilor purtate între diverse echipe, conform indicațiilor instructorului. Fiind bazată pe CLOUD, platforma va permite controlul unei game largi de resurse de calcul, stocare și rețea în cadrul unui centru de date. Infrastructura Open Source Cloud Computing trebuie să fie împărțit în servicii pentru a permite conectarea și lucrul cu componente ale bibliotecii, în funcție de nevoi.


CLOUD based platform




Ethernet switch
Two 25Gbps links
Two 25Gbps links
Two 25Gbps links
Two 25Gbps links
Two 25Gbps links
Two 25Gbps links
Two 25Gbps links
Two interlinks
NAS
Server 1
Server 2
Server 3
Server 4
Server 5
Server 6
Two 25Gbps links
Two 25Gbps links
Two 25Gbps links
Two 25Gbps links
Two 25Gbps links
Two 25Gbps links
Two 25Gbps links
Ethernet switch

Funcționalități ale echipamentului real:

3.	**Parametrii funcționali, tehnici și calitativi necesari:**
3.1.	Laboratorul Cyber trebuie să fie o soluție pur software, care ar trebui să fie independentă de orice componente hardware și ar trebui să fie gata să fie instalate și operaționale pe diferite medii independente, dacă cumpărătorul dorește acest lucru. Mediile pot fi: a. hardware furnizat de către contractant b. servere deținute de cumpărător c. Stații de lucru (PC/laptop-uri) ale cumpărătorului d. Servicii CLOUD, cum ar fi Azure sau AWS Instalarea pe mediile menționate mai sus nu face referire la software-ul de acces, ci la platforma de virtualizare în sine.
3.2.	Laboratorul Cyber include infrastructura hardware, echipamentele de infrastructură de rețea, platforma de virtualizare instalată, software-ul și hardware-ul specializat, necesare pentru organizarea exercițiilor și instruirii, precum și materialele de instruire.
3.3.	Laboratorul Cyber trebuie să fie permită utilizarea hardware-ul fizic și virtualizat, reproducând infrastructuri IT realiste, inclusiv tehnologii/infrastructuri tradiționale de calcul. Tehnologiile de virtualizare trebuie utilizate pe scară largă pentru a simula medii IT versatile în Laboratorul Cyber, fără a fi nevoie de prea multe componente fizice.
3.4.	Laboratorul Cyber trebuie să funcționeze eficient într-un mod autonom într-un mediu izolat (deconectat de la alte rețele), fără posibilitatea de conectare la Internet.
3.5.	Laboratorul Cyber nu ar trebui să trimită date pe Internet (adică capabilități de "comunicații multimedia") fără permisiunea cumpărătorului.
3.6.	Laboratorul Cyber trebuie să funcționeze eficient, cu suficiente resurse de calcul disponibile (CPU, RAM, transfer de rețea, stocare, etc.), pentru a sprijini un exercițiu de atac-apărare "live-fire" pentru cel puțin 10 echipe simultan, fiecare având cel puțin 30 membri și un segment de rețea care are mai puțin 30 de mașini virtuale pe echipă, fără întârzieri (delays) și timpi de răspuns (lags) notabile.
3.7.	Laboratorul Cyber trebuie să poată fi utilizat de cel puțin 300 de persoane reale conectate la platformă la nivel local sau prin conexiuni VPN, fără întârzieri (delays) și timpi de răspuns (lags) notabile.
3.8.	Laboratorul Cyber trebuie să fie complet accesibilă jucătorilor fără a instala software suplimentar pe stațiile de lucru (browser web).
3.9.	Laboratorul Cyber nu ar trebui să impună nicio limitare de software pentru scalabilitatea platformei, inclusiv numărul de utilizatori, numărul de mașini virtuale care rulează simultan în mediu.
3.10.	Scalabilitatea ar trebui să fie limitată doar de resursele hardware.
3.11.	Laboratorul Cyber trebuie să fie accesibil de pe Internet de către participanți, instructori și administratori printr-un canal securizat (de exemplu, tehnologie VPN sau similară) și controale de securitate adecvate pentru a permite accesul autorizat în mod explicit.
3.12.	Laboratorul Cyber va fi utilizat și va sprijini exerciții cibernetice naționale și internaționale și alte activități educaționale, cu accent principal pe scenariile de securitate cibernetică de apărare împotriva atacurilor într-un mediu semi-realist.
3.13.	Laboratorul Cyber trebuie să susțină următoarele tipuri de activități: - Exerciții cu scenarii de tip Atac-Apărare (Attack-defence scenario), cunoscute sub numele de "exerciții echipă roșu- echipă albastru" (red team-blue team exercises"); - Diferite scenarii/exerciții de răspuns la incidente și de apărare cibernetică (Cyber Defence) pentru instruirea persoanelor care răspund la incidente, inclusiv în domenii de apărare cibernetică (Cyber Defence), cum ar fi analiza amenințărilor (threat analysis), răspunsul la incidente (incident response), criminalistica digitală (digital forensics), etc.; - Exerciții de "capturarea steagului" (Capture the flag);

	- Sesiuni de instruire, cursuri, laboratoare și prelegeri; - Facilități Testing grounds. Soluțiile (hardware, software etc.) sunt testate pentru a vedea dacă funcționează corect. Laboratorul Cyber trebuie să ofere un mediu sigur pentru testarea instrumentelor COTS (software care rulează pe Linux/Windows, de preferință și dispozitive de rețea), artefacte și să colecteze IoCs. Testarea COTS implică o cantitate mare de teste a modului în care sistemul COTS comunică cu alte sisteme și surse de date prin interfețele sale. Indicatorii de compromis (IOCs) sunt diferite tipuri de date de securitate cibernetică care pot alerta organizațiile de iminența atacului rețelei lor, încălcări ale securității, infecții malware și incidente de securitate. - Conectarea componentelor fizice, cum ar fi Routere / switch-uri, dar și a altor componente; - Simularea infrastructurilor personalizate (real life like).
3.14.	Laboratorul Cyber trebuie să permită simularea: - Diferite scenarii de atac de nivel (level attack scenarios), de la cele simple până la cele avansate APT (advanced persistent threat); - Trebuie să susțină scenarii pentru participanți cu background diferit (e.g., ethical hacker, Cyber defenders, etc.) și diferite niveluri de expertiză (începători, intermediari, practicieni avansați, etc.); - Atac de tip zero-day malware, inclusiv ransomware, în diferite sisteme de operare; - Atac de tip Brute-force; - Data leakage/exfiltration; - Vulnerabilități și exploit-uri din partea clientului și a serverului. - Atacuri de tip Spams, phishing, and spear-phishing; - Domenii și site-uri rău intenționate, inclusiv site-uri de phishing - Atacuri de tip Denial-of-Service cu multiple variante (DDoS, RDoS, DRDoS)
3.15.	Laboratorul Cyber ar trebui să includă o bibliotecă de sisteme pre-construite, șabloane și scenarii de atac. Laboratorul Cyber ar trebui să aibă cel puțin 200 de imagini pre-construite ale mașinilor virtuale gata de a fi utilizate individual sau în scenariile de atac-apărare sau de antrenament. Mașinile virtuale ar trebui să includă, în mod specific, dar fără a le limita, diferite stații de lucru și servere Windows și Linux, cu diferite niveluri de vulnerabilități deja încorporate.
3.16.	Laboratorul Cyber ar trebui să ofere cel puțin 20 de scenarii de antrenament pre-construite, cu niveluri diferite de dificultate și atacuri în mai multe etape, care oferă cel puțin 6 ore de antrenament fiecare. Cel puțin câteva scenarii ar trebui să acopere vulnerabilitățile sistemelor de operare populare sau ale software-ului, cum ar fi: o Windows o Linux o Active Directory o Exchange
	Laboratorul Cyber ar trebui să furnizeze cel puțin 40 de infrastructuri statice pre-construite, care să semene cu rețelele corporative reale.
3.17.	Laboratorul Cyber ar trebui să ofere posibilitatea de a rula infrastructuri/instruiri pe termen nelimitat, dar și pe o perioadă limitată/stabilită de timp.
3.18.	Laboratorul Cyber ar trebui să ofere posibilitatea de a partaja mașini virtuale prin furnizarea unui link direct, cu posibilitatea de a urmări cu cine a fost partajat link-ul de către administrator. Link-ul ar trebui să aibă, de asemenea, o dată de expirare. După ce data de expirare a trecut, mașina nu trebuie să fie accesibilă sub linkul partajat, chiar dacă este încă online.
3.19.	Toate elementele bibliotecii (sisteme pre-construite, șabloane, scenarii de atac și alte elemente) ar trebui să fie complet personalizabile. Laboratorul Cyber ar trebui să permită pregătirea propriilor exerciții personalizate, scenarii, sesiuni de instruire prin utilizarea acestor elemente ale bibliotecii.

3.20.	Platforma de lucru utilizată in cadrul Laboratorului Cyber ar trebui să permită adăugarea de noi elemente de bibliotecă, personalizate, cum ar fi mașinile virtuale
3.21.	Laboratorul Cyber ar trebui să accepte formatele populare de imagine ale mașinii virtuale, dar nu limitat, cum ar fi: ***vdi, .ova, .vmdk, .vhdx, .vhd, .tar.gz, .tgz, .qcow2, .gz, .tar, .zip., .7z***, etc. Procesul de încărcare ar trebui să fie disponibil printr-o interfață grafică prin furnizarea unui link către un site extern care găzduiește imaginea dorită. Ar trebui să existe, de asemenea, o opțiune pentru a încărca o imagine din spațiul de stocare local.
3.22.	Laboratorul Cyber ar trebui să permită ***implementarea și resetarea rapidă*** (limitată în principal numai de transferul (throughput) hardware) a scenariilor pre-construite, reconstruirea mașinilor virtuale, scalarea și dublarea segmentelor de rețea pregătite dintr-o consolă administrativă centrală (central administrative dashboard). Totodată, trebuie să aibă o opțiune de resetare din fabrică care să permită începerea unei noi sesiuni de apărare cibernetică, de la zero (from scratch).
3.23	Laboratorul Cyber ar trebui să ofere o interfață prietenoasă (user-friendly) , intuitivă, ușor de utilizat, personalizabilă pentru a putea supraveghea și controla sesiunile de instruire, mecanismele de supraveghere și de evaluare a participanților și echipelor individuale și de generare și primire a rapoartelor de performanță ale echipelor.
3.24.	Laboratorul Cyber trebuie să furnizeze un rezumat automat al instruirii cursanților, împreună cu evaluarea automată a fiecărei sarcini a instruirii.
3.25	Laboratorul Cyber ar trebui să se bazeze pe principii de arhitectură deschisă, ceea ce înseamnă că mediul de instruire ar trebui să fie ușor de personalizat. Laboratorul Cyber trebuie să sprijine crearea de scenarii personalizate de atac și apărare, să personalizeze scenariile existente, ar trebui să permită adăugarea de mașini virtuale personalizate sau alte componente pe platformă.
3.26	Laboratorul Cyber trebuie să permită rularea diferitelor tehnologii de securitate și rețea de la diferiți furnizori de produse prezenți pe piață, inclusiv cele care sunt „simulate" (de exemplu, funcționează ca mașini virtuale) din domeniul Cybersecurity. ***Setul minim de tehnologii și produse de rețea și securitate*** care trebuie să fie prezente în mediul simulat CyberLab: o Routere (Network routers); o Switch-uri (Network switches); o Generator de trafic de rețea (Network traffic generator) – Laboratorul Cyber trebuie să includă capacități de generare a traficului în rețea pentru a simula traficul în rețea (legitim și rău intenționat). Generatorul de trafic de rețea oferit de contractant poate fi un dispozitiv fizic sau o soluție pur software. Generatorul de trafic de rețea ar trebui să accepte opțiuni de reglaj fin; o Rețelele simulate trebuie să reproducă rețele moderne comune (common modern enterprise networks), cu DMZ front-end și back-end, segmente de rețea interne dedicate serverelor și sistemelor client; o Firewall-uri de rețea: Cel puțin 2 de tehnologii diferite în cadrul rețelelor cibernetice simulate; o Tehnologii de monitorizare a securității rețelelor: Log Collection Engine, etc.; o Generarea de certificate VPN care permit accesul la mașinile virtuale și mediile de lucru.
3.27.	Laboratorul Cyber trebuie să permită crearea de grupe și/sau subgrupe de utilizatori. (Ex. Grupa A are 10 de utilizatori, putem crea subgrupa A1 și subgrupa A2, fiecare având câte 5 utilizatori din grupa A).
3.28.	Laboratorul Cyber trebuie să permită pregătirea inițială pentru grupele de lucru selectând dacă administratorul dorește să ofere o instruire pentru întreaga grupă sau instruire pentru fiecare utilizator/subgrupă din cadrul grupei principale.
3.29.	În cadrul Laboratorului Cyber trebuie să existe posibilitatea de a programa instruirea înainte de lansarea automată a componentelor ce fac obiectul instruirii.

3.30.	În cadrul Laboratorului Cyber trebuie să existe posibilitatea verificării resurselor de calcul disponibile administratorului, la intervalul de timp dorit, înainte de a accepta instruirea planificată. ***Ex.*** Platforma are capacitatea de a rula 10 de cursuri/sesiuni de instruire simultan. o Administratorul A a programat pentru ziua de luni 6 sesiuni de instruire între orele 10:00 și 1:00. o Administratorul B vrea să programeze 5 sesiuni de instruire pentru luni, de la ora 11. Platforma trebuie să-i permită administratorului B să știe că nu există suficiente resurse pentru a rula instruirea în acest moment și de asemenea, să calculeze câte cursuri/sesiuni de instruire poate rula în acest moment.
3.31.	În cadrul Laboratorului Cyber trebuie să existe posibilitatea conectării de dispozitive IoT și de a le integra cu mașinile virtuale.
3.32.	Laboratorul Cyber trebuie să ofere, de asemenea, posibilitatea de a configura dispozitivele în interfața grafică a platformei. Laboratorul Cyber trebuie să poată configura setările de rețea ale dispozitivelor fizice, împreună cu resetarea acestora la punctul de pornire al antrenamentului.
3.33.	Laboratorul Cyber trebuie să asigure capacitatea de conectare la alte dispozitivele fizice, utilizând standardul RJ45.
3.34	În cadrul Laboratorului Cyber trebuie să permită proceduri de recuperare a parolei pentru dispozitivele fizice în cazul unei parole uitate.
3.35.	Contractantul trebuie să livreze minim o ***instruire, de cel puțin 20 de ore***, pentru instructorii platformelor (până la 10 de participanți) de tip Cyber din cadrul ANMB, în termen de 4 săptămâni de la instalarea CyberLab-ului și să execute totodată si testul de stres de succes (successful stress test).
3.36	Contractantul trebuie să furnizeze: o documentul de proiectare CRP, care descrie soluția propusă (arhitectura tehnică), componentele sale și relația dintre acestea; o schema cu topologia posibilă; o elementele hardware (cantitățile) ale soluției propuse, precum și link-uri cu documentația producătorului și/sau documentația pe hârtie; o elementele software (cantitățile) ale soluției propuse, precum și link-uri cu documentația producătorului și/sau documentația pe hârtie;
3.37.	Software-ul utilizat în cadrul laboratorului Cyber trebuie să aibă o ***perioadă de suport de cel puțin 3 ani***, numărând de la data semnării actului de acceptare-transfer al platformei. În acest timp, contractantul trebuie să ofere ***acces la cele mai recente elemente de bibliotecă, mașini virtuale nou dezvoltate, noi scenarii de atac***, etc
3.38.	Echipamentul trebuie să vină cu toate licențele, software-ul, hardware-ul, cablurile etc., necesare pentru a oferi funcționalitatea specificată.

Structura IT pe care va rula aplicația software va avea minim următoarea componență:

A. HARDWARE ***Server (2x CPU, 1TB RAM, 6x1.92TB vSAS RI SSD, 2x16TB HDD SAS, RAID, 2x 10/25G LAN, 3Yr ProSupport –1 bucată cu următoarele cerințe:***	
Chassis Configuration	12X 3.5 SAS/SATA with XGMI and APERC on slot 2
Procesor	2 procesoare, minim Generația 2 cu 64 coruri/ procesor
RAM	Memory DIMM Type and Speed: 3200MT/s RDIMMs Minim 8 x DDR4 RDIMM (1TB), LRDIMM (2TB), bandwidth up to 3200 MT/S
HDD	• 6 x 1.92TB SSD vSAS Read Intensive 12Gbps 512e 2.5in w/3.5in HYB CARR ,AG Drive SED, 1DWPD; • 2 x 16TB HDD SAS 12Gbps 7.2K 512e 3.5in Hot-Plug

RAID Configuration	• Mixed Drive Types
RAID/Internal Storage Controllers	• Da
Fans	• 6 X Ventilator de înaltă performanță
OCP 3.0 Network Adapters	• 2 x Ethernet 10/25G LAN
Sursă alimentare	• Minim Dual, • Hot-Plug, Fully Redundant Power Supply (1+1), 1100W, Mixed Mode Titan
Rack Units	• 2U Rack Server
Bezel	• Optional LCD bezel or security bezel
Rack Rails	• Sliding Rails With Cable Management Arm
Server Accessories	• Fan Foam, HDD 2U
Securitate	• Cryptographically signed firmware • Secure Boot • Secure Erase • Silicon Root of Trust • System Lockdown (requires OpenManage Enterprise) • TPM 1.2/2.0, TCM 2.0 optional • Secure Memory Encryption (SME) • Secure Encrypted Virtualization (SEV)
B. SOFTWARE ***Cybersecurity CLOUD Apps, cerințe:***	

• Licență acces ***Cybersecurity CLOUD Apps*** (3 ani)
• Open Source Cloud Computing Infrastructure
• Open source relational database
• Software specializat:
  • Glance
  • Cinder
  • Keystone
  • Neutron
  • Nova
  • Horizon	

Anti Theft Device & Asset Tagging	• DA
***C.* RETEA DE DATE PENTRU INTERCONECTAREA ECHIPAMENTELOR:**	
• Orice fel de echipamente IT (rack, switch, mufe, etc.); • Cablurile de rețea; • Diverse materiale utilizate pentru mascarea cablurilor utilizate; • Alte materiale care sunt necesare pentru a realiza rețeaua de date	

Obligatoriu:

1. ***Ofertanții trebuie să își facă propriile măsurători pentru a stabili traseul pe care îl consideră optim în realizarea rețelei. Autoritatea contractantă nu va accepta să suplimenteze contractul cu materialele pe care ofertantul declarat câștigător nu a reușit să le prevadă în ofertă.***
2. ***Producătorul Laboratorului Cyber trebuie sa aparțină unui stat membru european sau SUA.***

3.3.2 Frecvența contractelor / termene de livrare / preț:

A. Contractele se vor încheia în conformitate cu datele din tabelul de mai jos:

Nr. crt.	Denumire produs	U/M	Cant.	Termen maxim de livrare	Termen maxim de montare, fixare / instalare / punere în funcțiune
1	**Laborator Cybersecurity (CyberLab)**	Cpl	1	În termen de ***maxim 120 zile*** de la semnarea contractului	În termen de ***maxim 30 zile*** de la livrarea produselor

3.3.3 Disponibilitate

Livrarea se va face în **maxim 120 zile de la data semnării contractului.**

Montare/instalare și punere în funcțiune - la sediul autorității contractante.

Termen de montare/instalare, punere în funcțiune și instruire personal – **maxim 30 zile de la livrarea *produselor.***

3.3.4 Garanție

Produsele trebuie să fie acoperite de garanție pentru ***cel puțin 2 ani de la data recepției (acceptării).***
Perioada de garanție începe de la data acceptării produselor sau în cazul amânării din cauze care nu țin de Contractant, la un interval de 15 zile de la acceptarea produselor.
Orice defecțiune / funcționare necorespunzătoare a produselor, precum și eventualele vicii ascunse vor fi sesizate în scris Contractantului, în termen de 48 de ore de la constatarea acestora de către Autoritatea contractantă.
Contractantul va remedia defecțiunea, funcționarea necorespunzătoare și/sau viciul ascuns în termen de maxim 5 zile de la data sesizării, fără costuri suplimentare pentru Autoritatea contractantă.
Garanția trebuie să acopere toate costurile rezultate din remedierea defectelor în perioada de garanție, inclusiv, dar fără a se limita la:

i.demontare, inclusiv închirierea de unelte speciale necesare pe durata intervenției (daca este aplicabil);
ii.ambalaje, inclusiv furnizarea de material protector pentru transport (carton, cutii, lăzi etc.);
iii.transport prin intermediul transportatorului, inclusiv de transport internațional (daca este aplicabil);
iv.diagnoza defectelor, inclusiv costurile de personal;
v.repararea tuturor componentelor defecte sau furnizarea unor noi componente;
vi.înlocuirea părților defecte;
vii.despachetarea, inclusiv curățarea spațiilor unde se efectuează intervenția;
viii.instalarea în starea inițială;
ix.testarea pentru a asigura funcționarea corectă;
x.repunerea în funcțiune.

3.3.5 Livrare, ambalare, etichetare, transport și asigurare pe durata transportului

Termenul de livrare este cel menționat la punctul ***3.3.2***. Un produs este considerat livrat când toate activitățile în cadrul contractului au fost realizate, produsul/echipamentul este montat, instalat/fixat în locația precizată, funcționează la parametrii agreați și este acceptat de Autoritatea contractantă.
Produsul va fi livrat cantitativ și calitativ la locul indicat de Autoritatea contractantă. Produsul va fi însoțit de toate subansamblele/părțile componente necesare montării, fixării, instalării, punerii și menținerii în funcțiune (după caz).
Contractantul va ambala și eticheta produsul furnizat astfel încât să prevină orice daună sau deteriorare în timpul transportului acestuia către destinația stabilită.

Dacă este cazul, ambalajul trebuie prevăzut astfel încât să reziste, fără limitare, manipulării accidentale, expunerii la temperaturi extreme, mediului salin și precipitațiilor din timpul transportului și depozitării în locuri deschise. În stabilirea mărimii și greutății ambalajului Contractantul va lua în considerare, acolo unde este cazul, distanța față de destinația finală a produselor furnizate și eventuala absență a facilităților de manipulare la punctele de tranzitare.

Transportul și toate costurile asociate sunt în sarcina exclusivă a contractantului. Produsele vor fi asigurate împotriva pierderii sau deteriorării intervenite pe parcursul transportului și cauzate de orice factor extern.

Destinația de livrare este cea comunicata la punctul 3.3.1.

Contractantul este responsabil pentru livrarea, montarea, instalarea, punerea în funcțiune (după caz) a produsului în termenul agreat și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu va invoca nici un motiv de întârziere sau costuri suplimentare.

3.3.6 Operațiuni cu titlu accesoriu

3.3.6.1 Montare, instalare, punere în funcțiune

Contractantul va monta, instala/fixa și va pune în funcțiune (după caz) produsele la locul de livrare indicat de Autoritatea contractantă și va efectua orice altă configurație considerată necesară pentru a asigura funcționalitatea produselor, în termenele stabilite la **pct. 3.3.2 din Caietul de sarcini**.

Contractantul trebuie să monteze, instaleze/fixeze și să pună în funcțiune (după caz) toate produsele în mod corespunzător, asigurând-se în același timp ca spațiile unde s-au realizat aceste operațiuni rămân curate. După livrarea, montarea, instalarea/fixarea și punerea în funcțiune a produselor, contractantul va elimina toate deșeurile rezultate și va lua măsurile adecvate pentru a aduna toate ambalajele și eliminarea acestora din spațiile Autorității contractante.

3.3.6.2 Instruirea personalului pentru utilizare

La momentul instalării și punerii în funcțiune, operatorul economic trebuie să asigure instruirea pentru un număr minim de ***10 instructori*** din cadrul ANMB. Această instruire se va organiza pe o durată de ***minim 20 ore***, de preferință, în funcție de nevoile de pregătire ale achizitorului, în urma unei planificări stabilite în prealabil de către achizitor și prestator și va cuprinde, dar nu se va limita la următoarele aspecte:

- prezentarea tuturor funcționalităților Laboratorului Cyber;
- modul de creare/ dezvoltare a exercițiilor;
- subiecte de interes pentru instructorii achizitorului, înaintate în prealabil către prestator, în funcție de necesitățile acestora;
- exemple de bună practică în ceea ce privește utilizarea software-ului Laboratorului Cyber.

Prestatorul va asigura eliberarea de certificate de competență pentru instructorii din cadrul ANMB.

3.3.6.3 Mentenanța preventivă în perioada de garanție

Contractantul va pune la dispoziția Autorității contractante - Instrucțiuni de mentenanță preventivă în perioada de garanție (inclusiv ritmicitatea operațiunilor).

Operațiunile de mentenanță preventivă a echipamentelor cuprind o serie de activități planificate și riguroase menite să le mențină în perfectă stare de funcționare și să optimizeze eficiența acestora în conformitate cu specificațiile tehnice ale echipamentului. În plus, scopul acestor operațiuni este de a extinde durata lor de viață, de a evita situațiile care pot perturba activitatea Autorității Contractante și de a minimiza posibilitatea unei defecțiuni precum și asigurarea unui consum minim de energie.

Contractantul este responsabil pentru realizarea operațiunilor de mentenanță preventivă (în conformitate cu cerințele stabilite de către producătorul echipamentului, așa cum au fost agreate de părți conform contractului și caietului de sarcini).

Orele de lucru normale ale Autorității Contractante sunt de la 07:30 la 15:30, de luni până vineri. Operațiunile de mentenanță preventivă care necesită o oprire a echipamentelor se efectuează în afara orelor normale de activitate. Datele exacte vor fi agreate cu Autoritatea Contractantă.
După fiecare intervenție preventivă, Contractantul trebuie să efectueze teste de funcționare ale echipamentului.

3.4. Mediul în care este operat produsul

Produsele vor fi operate în facultățile din cadrul Academiei Navale "Mircea cel Bătrân", în încăperi ventilate și racordate la rețeaua de termoficare (în sezonul rece).
Constrângeri privind locația unde se va efectua livrarea/instalarea – nu este cazul.

4. Documentații ce trebuie furnizate Autorității contractante în legătură cu produsul

Nr. crt.	Documentații furnizate de Contractant	Termen limită de punere la dispoziție
1	Fișa/cartea tehnică a produsului	cel mai târziu la data livrării
2	Instrucțiuni de cunoaștere și exploatare în limba română care să cuprindă cel puțin documentația de cunoaștere și exploatare	
3	Instrucțiuni de mentenanță preventivă	
4	Inventarul de complet cantitativ și valoric (lista tuturor ansamblelor, subansamblelor, pieselor componente, pentru fiecare sistem/complet)	
5	Instrucțiuni de utilizare și întreținere (emise de producător), care detaliază, minimal, modul de utilizare și de întreținere a produselor	
6	Manual de întreținere în limba română	

NOTĂ: Toate documentațiile vor fi în limba română și engleză.

5. Recepția produselor

Recepția produselor se va efectua pe bază de proces-verbal semnat de Contractant și Autoritatea contractantă.
Recepția se va realiza în două etape, respectiv:

- recepția cantitativă - prin numărarea bucată cu bucată (piesă cu piesă) a ansamblelor, subansamblelor, pieselor componente și prin compararea cu datele înscrise în avizul de expediție (dacă este cazul), în inventarul de complet și în ofertă – ***în maxim 1 zi de la livrare***;
- recepția calitativă - punerea în funcțiune, verificarea funcționării și înregistrării parametrilor, pentru fiecare produs livrat, conform specificațiilor tehnice, remedierea eventualelor defecte constatate și acceptarea produsului – ***în maxim 5 zile de la recepția cantitativă.***

Recepția calitativă va include unul din următoarele rezultate:

a) acceptat;
b) acceptat cu observații minore;
c) acceptat cu rezerve;
d) refuzat.

Criteriile referitoare la rezultatul recepției calitative, numărul și tipul defectelor identificate, precum și termenul de remediere, sunt detaliate în tabelul următor:

Rezultatul recepției calitative	Numărul defectelor identificate	Termen de remediere
Acceptat	-	-
Acceptat cu observații	1-3	5 zile
Acceptat cu rezerve	4-5	7 zile
Refuzat	> 5	10 zile

6. Modalități si condiții de plata

Contractantul va emite factură fiscală pentru produsele livrate. Fiecare factură va avea menționat numărul contractului, datele de emitere și de scadență ale facturii respective. Facturile vor fi trimise în original la sediul Autorității contractante numai după semnarea procesului verbal de recepție, prin care se confirmă livrarea, recepția și acceptarea produselor (montarea, instalarea/fixarea, punerea în funcțiune și remedierea eventualelor defecte constatate – după caz).

Procesul verbal de recepție va însoți factura și reprezintă elementul necesar realizării plății, împreună cu celelalte documente justificative prevăzute mai jos:

- factură fiscală;
- certificat de garanție;
- documentațiile prevăzute la pct. 4 al Caietului de sarcini

Plățile în favoarea Contractantului se vor efectua în ***termen de 30 de zile de la data emiterii facturii fiscale*** în original și a tuturor documentelor justificative.

7. Obligațiile principale ale Autorității contractante

Autoritatea contractantă va pune la dispoziția Contractantului, cu promptitudine, orice informații și/sau documente pe care le deține și care pot fi relevante pentru realizarea Contractului. În măsura în care Autoritatea contractantă nu furnizează datele/informațiile/documentele solicitate de către Contractant, termenele stabilite în sarcina Contractantului pentru furnizarea produselor se prelungesc în mod corespunzător.

Autoritatea contractantă se obligă să respecte dispozițiile din prezentul Caiet de sarcini.

Autoritatea contractantă își asumă răspunderea pentru veridicitatea, corectitudinea și legalitatea datelor/informațiilor/documentelor puse la dispoziția Contractantului în vederea îndeplinirii Contractului. În acest sens, se prezumă că toate datele/informațiile/documentele prezentate Contractantului sunt însușite de către conducătorul unității și/sau de către persoanele în drept având funcție de decizie care au aprobat respectivele documente.

Autoritatea contractantă va colabora, atât cât este posibil, cu Contractantul pentru furnizarea informațiilor pe care acesta din urmă le poate solicita în mod rezonabil pentru realizarea Contractului.

Autoritatea contractanta are obligația să desemneze, în termen de 5 zile de la semnarea contractului, persoana de contact.

Autoritatea Contractantă se obligă să recepționeze produsele furnizate și să certifice conformitatea astfel cum este prevăzut în prezentul Caiet de sarcini.

Autoritatea Contractantă poate notifica Contractantul cu privire la necesitatea revizuirii/respingerea produselor. Solicitarea de revizuire/respingerea va fi motivată, cu comentarii scrise.

Autoritatea contractantă are dreptul de a rezoluționa/rezilia contractul atunci când se respinge produsul livrat, de două ori, pe motive de calitate.

Recepția produselor se va realiza conform procedurii prevăzute în prezentul Caiet de sarcini.

Autoritatea contractantă se obligă să plătească prețul contractului către Contractant, în termen de maximum 30 de zile de la data înregistrării facturii în original la sediul Achizitorului și a documentelor justificative menționate în prezentul Caiet de sarcini.

8. Cadrul legal care guvernează relația dintre Autoritatea contractantă și Contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă)

Ofertantul devenit Contractant are obligația de a respecta în executarea Contractului, obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii, prin dreptul național, prin acorduri colective sau prin dispozițiile internaționale de drept în domeniul mediului, social și al muncii enumerate în anexa X la Directiva 2014/24, respectiv:

i. Convenția nr. 87 a OIM privind libertatea de asociere și protecția dreptului de organizare;
ii. Convenția nr. 98 a OIM privind dreptul de organizare și negociere colectivă;
iii. Convenția nr. 29 a OIM privind munca forțată;

iv. Convenția nr. 105 a OIM privind abolirea muncii forțate;
v. Convenția nr. 138 a OIM privind vârsta minimă de încadrare în muncă;
vi. Convenția nr. 111 a OIM privind discriminarea (ocuparea forței de muncă și profesie);
vii. Convenția nr. 100 a OIM privind egalitatea remunerației;
viii. Convenția nr. 182 a OIM privind cele mai grave forme ale muncii copiilor;
ix. Convenția de la Viena privind protecția stratului de ozon și Protocolul său de la Montreal privind substanțele care epuizează stratul de ozon;
x. Convenția de la Basel privind controlul circulației transfrontaliere a deșeurilor periculoase și al eliminării acestora (Convenția de la Basel);
xi. Convenția de la Stockholm privind poluanții organici persistenți (Convenția de la Stockholm privind POP);

9. Managementul/Riscuri/Gestionarea contractului și activități de raportare în cadrul contractului

Riscuri posibile	Modalitate de eliminare a riscului
Nesemnarea contractului de ofertantul câștigător	Anunțarea ofertantului calificat pe locul următor
Neconstituirea garanției de bună execuție	Nerestituirea garanției de participare
Menținerea unei legături defectuoase între cele două părți semnatare ale contractului	Nominalizarea unor persoane responsabile pentru monitorizarea contractului
Întârzieri în livrarea produselor	Nominalizarea unui responsabil de contract pentru monitorizarea desfășurării contractului
Livrarea unor produse inferioare față de cele ofertate în propunerea tehnică	În momentul executării recepției se va verifica corespondența specificațiilor tehnice ale produselor livrate cu cele din propunerea tehnică și caietul de sarcini
Defecte de fabricație semnalate în timpul utilizării produselor	Menționarea în contract a perioadei de garanție ofertată.

Notă:

Specificațiile tehnice care indică o anumită origine, sursă, producție, un procedeu special, o marcă de fabrică sau de comerț, o licență de fabricație sunt menționate doar pentru identificarea cu ușurință a tipului de produs ce urmează a fi achiziționat și nu au ca efect favorizarea sau eliminarea anumitor operatori economici. Aceste specificații vor fi interpretate ca având mențiunea „sau echivalent".

În cazul în care pe parcursul îndeplinirii contractului se constată că anumite elemente ale propunerii tehnice sunt inferioare sau nu corespund cerințelor prevăzute în caietul de sarcini, prevalează prevederile caietului de sarcini.

Întocmit,
Șef birou achiziții
Lt. Cdor Schipor Constantin

Specialist Departament Sisteme Electromecanice Navale
Lect.univ.dr.ing. Florin POSTOLACHE

Verificat concordanța prevederilor Caietului de sarcini cu necesitățile obiective ale Academiei Navale „Mircea cel Bătrân",
Cdor
Paul BURLACU