Date of Issue: 29/01/2025
Salvage and Marine Operations

[redacted]
Defence Equipment & Support
SALMO Team
Ash 2A #3212
MOD Abbey Wood
Bristol
BS34 8JH

For the attention of:

Our Ref: 713539451 –
HMS CASSANDRA Wreck Survey
DCCP: RAR 250116A07
DPIA: P332171

ITT NUMBER & TITLE: 713539451 - HMS CASSANDRA Wreck Survey

1. On behalf of the Secretary of State for Defence, I hereby give you notice of the information or assets connected with, or arising from, the referenced ITT that constitute classified material.

2. Aspects that constitute classified material, including UK OFFICIAL-SENSITIVE for the purpose of DEFCON 660, are specified below. These aspects must be fully safeguarded. The enclosed "Security Conditions" outlines the minimum measures required to safeguard UK OFFICIAL SENSITIVE assets and information.

ASPECTS	CLASSIFICATION
Sharing of information regarding the Authority contract to any third-party suppliers	OFFICIAL SENSITIVE
Information that is disclosed orally in confidence by Authority (DEFCON 531, Para 10 applies – Nothing in this condition shall affect the parties' obligations of confidentiality where information is discussed orally in confidence).	OFFICIAL SENSITIVE
Systems design documents specific to the Authority (Such as Statements of technical requirements or Non-COTS equipment specifications.)	OFFICIAL SENSITIVE
Contract documentation including tender document, costings, and Commercial Strategy.	OFFICAL SENSITIVE
Project delivery schedule and associated milestones. Project delivery meeting minutes/ROADS.	OFFICAL SENSITIVE

Project deliverables including associated Security, Engineering and Support documentation.	OFFICIAL SENSITIVE
System Test information, data sets and records/results including limitations and performance metrics specific to the Authority, and the Authority vessel	OFFICIAL SENSITIVE
Hardware or Software Code containing security enforcing functionality	OFFICIAL SENSITIVE
Personal details of Authority staff, Contractors, and System Operators	OFFICAL SENSITIVE

3. You are required to complete a Supplier Assurance Questionnaire (SAQ) against the Defence Cyber Protection Partnership (DCPP) Risk Assessment Reference (RAR). Please use the attached SAQ Form and return to: UKStratComDD-CyDR-DCPP@mod.gov.uk

4. Measures must be taken to safeguard classified information and assets in accordance with applicable national laws and regulations. Your attention is drawn to the requirements of the Security Conditions. You should take all reasonable steps to make sure that all individuals employed on any work in connection with the ITT that have access to classified information and assets are aware of the protective requirements and that such requirements will continue to apply should the ITT be unsuccessful.

5. Will you please confirm that:

a. This definition of the classified aspects of the referenced Invitation to Tender has been brought to the attention of the person directly responsible for security of classified material.

b. The definition is fully understood.

c. Measures can, and will, be taken to safeguard the classified aspects identified herein in accordance with applicable national laws and regulations. [The requirement and obligations set out above and in any contractual document can and will be met and that the classified information shall be protected in accordance with applicable national laws and regulations.]

6. If you have any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will you please let me know immediately.

7. Classified Information associated with this ITT must not be published or communicated to anyone without the approval of the MOD Contracting Authority.

8. Any access to classified information or assets on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Officer in accordance with DEFCON 76.

Yours faithfully

[redacted]

Copy via email to:
ISAC-Group (MULTIUSER)
COO-DSR-IIPCSy (MULTIUSER)
UKStratComDD-CyDR-CySAAS-021

Annex:

A. Acceptance of Salmo Security Aspects Letter (SAL)

Enclosures:

1. OFFICIAL SENSITIVE Security Condition for UK Contracts.
2. DEFCON 660, EDN 12/15
3. DEFCON 531 EDN 09/21 Disclosure of Information
4. DEFCON 76 EDN 11/22 Contractors Personnel at Government Establishments.

ANNEX A TO SAL:
ITT/CONTRACT NUMBER & TITLE: 713539451 - HMS CASSANDRA Wreck Survey
DATED: 29/01/2025

FOA: [redacted],
[redacted],
Defence Equipment and Support (DE&S),
SALMO Team,
MoD ABBEY WOOD,
ASH 2B #3212,
BRISTOL,
BS34 8JH.

ACCEPTANCE OF SALMO SECURITY ASPECTS LETTER (SAL)

Receipt of the above **713539451 - HMS CASSANDRA Wreck Survey** dated **29/01/2025** is acknowledged and understood.

On behalf of the Contractor, I confirm that:

a. The SAL is understood and all personnel (as defined within the contract) who require access to Government Identifiable Information have been briefed on the security requirements in this SAL, and meet the security and access requirements, including 'need to know', clearance and nationality.

b. The definitions of OFFICIAL-SENSITIVE Matter of the above contract, and all the security requirements in this SAL, have been brought to the attention of the person directly responsible for the security of this contract. This will include supplying suitable cascaded SALs and references to subcontractors,

c. Individual need to know and access requirements in relation to DELIVERABLE, are strictly role-based, and therefore automatically rescinded on job change or departure and procedures will be taken to maintain this requirement.

d. All conditions and requirements in this SAL will be complied with.

Signed: [redacted] Date: 4 March 2025

Name: [redacted] Job Title [redacted]

ENCLOSURE 1 TO
SAL 713539451 - HMS CASSANDRA Wreck Survey
DATED 29/01/2025

Issued 15 April 2024

UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS

Purpose

1. This document provides guidance for Defence Suppliers where classified material provided to or generated by the Defence Supplier is graded UK OFFICIAL or UK OFFICIAL-SENSITIVE. Where the measures requested below cannot be achieved or are not fully understood, further advice should be sought from the UK Designated Security Authority (Email: COO-DSR-IIPCSy@mod.gov.uk).

Definitions

2. The term "Authority" for the purposes of this Annex means the UK MOD Contracting Authority.

1. The term "Classified Material" for the purposes of this Annex means classified information and assets.

Security Grading

2. The SENSITIVE marking is used to denote UK OFFICIAL material that is of a particular sensitivity and where there is a need to reinforce the 'need to know'. The Security Aspects Letter, issued by the Authority shall define the UK OFFICIAL-SENSITIVE material that is provided to the Defence Supplier, or which is to be developed by it, under this Contract. The Defence Supplier shall mark all UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security grading. The Defence Supplier is not required to mark documents graded UK OFFICIAL unless they are transmitted overseas or generated by a Defence Supplier based outside the UK in a third-party country.

Security Conditions

3. The Defence Supplier shall take all reasonable steps to adhere to the provisions specified in the Contract or listed in this Annex. The Defence Supplier shall make sure that all individuals employed on any work in connection with the Contract have notice that these provisions apply to them and shall continue so to apply after the completion or earlier termination of the Contract.

4. Where a Defence Supplier is based outside the UK in a third-party country the national rules and regulations of the third-party country take precedence over these conditions only if the third-party country has an extant bilateral security agreement or arrangement with the UK.

5. The Authority shall state the data retention periods to allow the Defence Supplier to produce a data management policy.

6. If you are a Defence Supplier located in the UK, your attention is also drawn to the provisions of the Official Secrets Act 1989 and the National Security Act 2023.

Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Classified Material

7. The Defence Supplier shall protect UK OFFICIAL and UK OFFICIAL-SENSITIVE material provided to or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Defence Supplier shall take all reasonable steps to prevent the loss or compromise of classified material whether accidentally or from deliberate or opportunist attack.

8. Once the Contract has been awarded, where the Defence Supplier is required to store or process UK MOD classified information electronically, they shall comply with the requirements specified in ISNs, Defence Condition 658 and Defence Standard 05-138. Details can be found at the links below:

https://www.gov.uk/government/publications/industry-security-notices-isns
https://www.dstan.mod.uk/toolset/05/138/000003000.pdf
https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down

9. All UK classified material including documents, media and other assets shall be physically secured to prevent unauthorised access. When not in use UK classified material shall be handled with care to prevent loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE material shall be stored under lock and key and shall be placed in a lockable room, cabinets, drawers or safe and the keys/combinations shall be controlled.

10. Disclosure of UK classified material shall be strictly controlled in accordance with the "need to know" principle. Except with the written consent of the Authority, the Defence Supplier shall not disclose the Contract or any provision thereof to any person other than to a person directly employed by the Defence Supplier or Subcontractor.

11. Except with the consent in writing of the Authority the Defence Supplier shall not make use of the Contract or any classified material issued or provided by or on behalf of the Authority otherwise than for the purpose of the Contract, and, same as provided for in paragraph 9 above, the Defence Supplier shall not make use of any article or part thereof similar to the articles for any other purpose.

12. Subject to any intellectual property rights of third parties, nothing in this Security Condition shall restrict the Defence Supplier from using any specifications, plans, drawings and other documents generated outside of this Contract.

13. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and shall be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 39.

Access

14. Access to UK classified material shall be confined to those individuals who have a “need-to-know”, have been made aware of the requirement to protect the material and whose access is essential for the purpose of their duties.

15. The Defence Supplier shall ensure that all individuals requiring access to UK OFFICIAL and UK OFFICIAL-SENSITIVE material have undergone basic recruitment checks. This should include establishing proof of identity; confirming that they satisfy all legal requirements for employment by the

16. Defence Supplier; and verification of their employment record. Criminal record checks should also be undertaken where permissible under national/local laws and regulations. This is in keeping with the core principles set out in the UK Government (HMG) Baseline Personnel Security Standard (BPSS) which can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf

Hard Copy Distribution

17. UK OFFICIAL and UK OFFICIAL-SENSITIVE documents may be distributed internally and externally of Defence Supplier premises. To maintain confidentiality, integrity and availability, distribution shall be controlled such that access to documents is only by authorised personnel. They may be sent by ordinary post in a single envelope. The words UK OFFICIAL or UK OFFICIAL-SENSITIVE must not appear on the envelope. The envelope must bear a stamp or marking that clearly indicates the full address of the office from which it was sent. Commercial Couriers may be used.

18. Advice on the distribution of UK OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of UK OFFICIAL-SENSITIVE shall be sought from the Authority.

Electronic Communication and Telephony and Facsimile Services

19. UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a National Cyber Security Centre (NCSC) Commercial Product Assurance (CPA) cryptographic product or a UK MOD approved cryptographic technique such as Transmission Layer Security (TLS). In the case of TLS both the sender and recipient organisations must have TLS enabled. Details of the required TLS implementation and CPA scheme are available at:

https://www.ncsc.gov.uk/guidance/tls-external-facing-services
https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

20. Exceptionally, in urgent cases UK OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so, but only with the prior approval of the Authority. However, it shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the Authority require. Such limitations including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the information.

21. UK OFFICIAL and UK OFFICIAL-SENSITIVE information may be discussed verbally on corporate telephones and other corporate electronic devices with persons located both within the country of the Defence Supplier and overseas. UK OFFICIAL-SENSITIVE information should only be discussed where there is a strong business need to do so.

22. UK OFFICIAL information may be faxed to recipients located both within the country of the Defence Supplier and overseas, however UK OFFICIAL-SENSITIVE information may be transmitted only where there is a strong business case to do so and only with the prior approval of the Authority.

Use of Information Systems

23. The detailed functions that must be provided by an IT system to satisfy the minimum requirements cannot all be described here in specific detail; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

24. The Defence Supplier should ensure 10 Steps to Cyber Security (Link below) is applied in a proportionate manner for each IT and communications system storing, processing or generating UK OFFICIAL or UK OFFICIAL-SENSITIVE information.

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

25. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum security requirements for processing and accessing UK OFFICIAL and UK OFFICIAL-SENSITIVE information on IT systems.

a. Access. Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of “least privilege” will be applied to System Administrators. Users of the IT System (Administrators) should not conduct ‘standard’ User functions using their privileged accounts.

b. Identification and Authentication (ID&A). All systems are to have the following functionality:

(1) Up-to-date lists of authorised users.

(2) Positive identification of all users at the start of each processing session

c. Passwords. Passwords are part of most ID&A security measures. Passwords are to be “strong” using an appropriate method to achieve this, e.g., including numeric and “special” characters (if permitted by the system) as well as alphabetic characters.

d. Internal Access Control. All systems are to have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission. Unless the Authority authorises otherwise, UK OFFICIAL-SENSITIVE information may only be transmitted or accessed electronically (e.g., point to point computer links) via a public network like the Internet, using a CPA product or equivalent as described in paragraph 20 above.

f. Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.

(1) The following events shall always be recorded:

(a) All log on attempts whether successful or failed,
(b) Log off (including time out where applicable),
(c) The creation, deletion or alteration of access rights and privileges,
(d) The creation, deletion or alteration of passwords.

(2) For each of the events listed above, the following information is to be recorded:

(a) Type of event,
(b) User ID,
(c) Date & Time,
(d) Device ID.

(3) The accounting records are to have a facility to provide the System Manager with a hard copy of all or selected activity. There also must be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know. If the operating system is unable to provide this, then the equipment must be protected by physical means when not in use i.e., locked away or the hard drive removed and locked away.

g. Integrity & Availability. The following supporting measures are to be implemented:

(1) Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g., viruses and power supply variations),

(2) Defined Business Contingency Plan,

(3) Data backup with local storage,

(4) Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software),

(5) Operating systems, applications and firmware should be supported,

(6) Patching of Operating Systems and Applications used are to be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.

h. Logon Banners. Wherever possible, a “Logon Banner” will be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring. A suggested format for the text (depending on national legal requirements) could be: “Unauthorised access to this computer system may constitute a criminal offence”.

i. Unattended Terminals. Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

j. Internet Connections. Computer systems must not be connected direct to the Internet or “un-trusted” systems unless protected by a firewall (a software based personal firewall is the minimum, but risk assessment and management must be used to identify whether this is sufficient).

k. Disposal. Before IT storage media (e.g., disks) are disposed of, an erasure product must be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

Portable Electronic Devices

26. Portable Electronic Devices holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 20 above.

27. Unencrypted Portable Electronic Device and drives containing personal data are not to be taken outside of secure sites1. For the avoidance of doubt the term “drives” includes all removable, recordable media e.g., memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.

28. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

29. Portable Electronic Devices holding the Authorities’ data are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the Portable Electronic Device is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

Loss and Incident Reporting

30. The Defence Supplier shall immediately report any loss or otherwise compromise of any Defence Related Classified Material to the Authority. The term Defence Related Classified Material includes any information or asset that has been given a security classification by the UK MOD. The term also includes classified information and assets held by UK Defence Suppliers which are owned by a third party e.g., NATO or another country for which the UK MOD is responsible.

31. In addition, any loss or otherwise compromise of Defence Related Classified Material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP). This will assist the UK MOD in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD’s Chief Information Officer (CIO) and, as appropriate, the Defence Supplier concerned. The UK MOD Defence Industry WARP will also advise the Defence Supplier what further action is required to be undertaken.

UK MOD Defence Industry WARP Contact Details
Email: DefenceWARP@mod.gov.uk (OFFICIAL with no NTK restrictions)
RLI Email: defencewarp@modnet.r.mil.uk (MULTIUSER)
Telephone (Office hours): +44 (0) 3001 583 640
Mail: Defence Industry WARP, DE&S PSyA Office
MOD Abbey Wood, NH2 Poplar-1 #2004, Bristol, BS34 8JH

32. Reporting instructions for any security incidents involving Defence Related Classified Material can be found in the Incident Reporting Industry Security Notice at:

https://www.gov.uk/government/publications/industry-security-notices-isns

Subcontracts

33. Where the Defence Supplier wishes to subcontract any elements of a Contract to Subcontractors within its own country or to Subcontractors located in the UK such subcontracts will be notified to the

[1] Secure Sites are defined as either Government premises or a secured office on the Defence Supplier premises.

Authority. The Defence Supplier shall ensure that these Security Conditions are incorporated within the subcontract document.

34. The prior approval of the Authority shall be obtained should the Defence Supplier wish to subcontract any UK OFFICIAL-SENSITIVE elements of the Contract to a Subcontractor facility located in another (third party) country. The first page of MOD Form 1686 (F1686) is to be used for seeking such approval. The MOD Form 1686 can be found in the "Subcontracting or Collaborating on Classified MOD Programmes ISN" at the link below:

https://www.gov.uk/government/publications/industry-security-notices-isns

35. If the subcontract is approved, the Defence Supplier shall flow down the Security Conditions in line with paragraph 34 above to the Subcontractor. Defence Suppliers located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

Physical Destruction

36. As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when the classified material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Defence Supplier to be necessary or desirable. Unwanted UK OFFICIAL-SENSITIVE classified material which cannot be destroyed in such a way shall be returned to the Authority.

Private Venture Activities

37. Private Venture (PV) funded (i.e., non-MOD funded) defence related projects and technology fall within one of the following three categories:

a. Variants. Variants of standard defence equipment under research, development or in production, e.g., aircraft, military vehicles or ships, etc. with non-standard equipment or fitments, offered to meet special customer requirements or to avoid security or commercial difficulties associated with the sale of an item in-Service with UK Armed Forces.

b. Derivatives. Equipment for military or civil use that is not based on standard Service designs but is dependent upon expertise or technology acquired in the course of defence contracts.

c. Freelance. Equipment of defence importance that is in no way based on information gained from defence contracts.

38. UK Defence Suppliers shall ensure that any PV activity that falls into one of the above categories has been formally security graded by the MOD Directorate of Security and Resilience. Please see PV guidance on the following website further information:

https://www.gov.uk/government/publications/private-venture-pv-grading-and-exhibition-clearance-information-sheets

Publicity Material

39. Defence Suppliers wishing to release any publicity material or display assets that arises from a Contract to which these Security Conditions apply must seek the prior approval of the Authority. Publicity material includes open publication in the Defence Supplier's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the UK Government.

40. For UK Defence Suppliers where the exhibition assets relate to multiple Delivery Teams or for Private Venture defence related classified material where there is no defined Delivery Team, the Defence Supplier shall request clearance for exhibition from the Directorate of Security and Resilience. See the MOD Exhibition Guidance on the following website for further information:

https://www.gov.uk/government/publications/private-venture-pv-grading-and-exhibition-clearance-information-sheets

Export sales/promotion

41. The MOD Form 680 (F680) security procedure enables MOD to control when, how, and if defence related classified material is released by UK Defence Suppliers to foreign entities for the purposes of promotion or sales of equipment or services. Before undertaking any targeted promotion or demonstration or entering into any contractual commitments involving the sale or release of defence equipment, information or technology classified UK OFFICIAL-SENSITIVE or above to a foreign entity, a UK Defence Supplier shall obtain F680 approval from the Export Control Joint Unit (ECJU) MOD Team. This includes assets classified UK OFFICIAL-SENSITIVE or above either developed to meet a UK MOD requirement or Private Venture (PV) equipment, as formally advised in a Security Aspects Letter (SAL) issued by the relevant Authority, or PV Security Grading issued by the MOD Directorate of Security and Resilience. Guidance regarding the F680 procedure issued by ECJU can be found at:

https://www.gov.uk/government/publications/ministry-of-defence-form-680-procedure-guidance

42. If a Defence Supplier has received an approval to subcontract, under an MOD Form 1686 (F1686), for development/production of parts of an equipment, that approval also permits the production of additional quantities for supply to an export customer, when the Defence Supplier has MOD Form 680 approval for supply of the complete equipment, as long as:

a. they are identical, except for component obsolescence, to items produced under the UK programme that the approval to subcontract relates to; and

b. no additional OFFICIAL-SENSITIVE or above material is required to be released to the overseas Subcontractor.

Interpretation/Guidance

43. Advice regarding the interpretation of the above requirements should be sought from the Authority.

44. Further requirements, advice and guidance for the protection of UK classified material at the level of UK OFFICIAL and UK OFFICIAL-SENSITIVE may be found in Industry Security Notices at:

https://www.gov.uk/government/publications/industry-security-notices-isns

Audit

45. Where considered necessary by the Authority the Defence Supplier shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Defence Supplier's processes and facilities by representatives of the Defence Supplier's National/Designated Security Authorities or the Authority to ensure compliance with these requirements.

ENCLOSURE 2 TO
SAL 713539451 - HMS CASSANDRA Wreck Survey
DATED 29/01/2025

DEFCON 660 (Edn 12/15) **Official-Sensitive Security Requirements**

1. In this condition “information” means information recorded in any form disclosed or created in connection with the contract.
2. The contractor shall protect all information relating to the aspects designed OFFICIAL- SENSITIVE as identified in the security aspects letter annexed to the contract, in accordance with the security conditions contained in the contract or annexed to the Security Aspects Letter.
3. The contractor shall include the requirements and obligations set out in clause 2 in any-subtract placed in connection with or for the purposes of the Contract which requires disclosure of OFFICIAL- SENSITIVE Information to the subcontractor or under which any information relating to aspects designated as OFFICIAL- SENSITIVE is created by the subcontractor. The Contractor shall also include in the sub-contract a requirement of this clause to the lowest level where any OFFICIAL- SENSITIVE Information is handled.

ENCLOSURE 3 TO
SAL 713539451 - HMS CASSANDRA Wreck Survey
DATED: 29/01/2025

DEFCON 531 (Edition 09/21) **Disclosure of Information**

1. 'Information' means any information in any written or other tangible form disclosed to one party by or on behalf of the other party under or in connection with the Contract, including information provided in the tender or negotiations which preceded the award of the Contract.

2. Subject to Clauses 5 to 10 each party:

a. shall treat in confidence all Information it receives from the other;

b. shall not disclose any of that Information to any third party without the prior written consent of the other party, which consent shall not unreasonably be withheld, except that the Contractor may disclose Information in confidence, without prior consent, to such persons and to such extent as may be necessary for the performance of the Contract;

c. shall not use any of that Information otherwise than for the purpose of the Contract; and

d. shall not copy any of that Information except to the extent necessary for the purpose of exercising its rights of use and disclosure under the Contract.

3. The Contractor shall take all reasonable precautions necessary to ensure that all Information disclosed to the Contractor by or on behalf of the Authority under or in connection with the Contract:

a. is disclosed to their employees and sub-contractors, only to the extent necessary for the performance of the Contract; and

b. is treated in confidence by them and not disclosed except with prior written consent or used otherwise than for the purpose of performing work or having work performed for the Authority under the Contract or any subcontract under it.

4.The Contractor shall ensure that their employees are aware of their arrangements for discharging the obligations at Clauses 2 and 3 before they receive Information and take such steps as may be reasonably practical to enforce such arrangements.

5. A party shall not be in breach of Clauses 2, 3, 7, 8 and 9 to the extent that either party:

a. exercises rights of use or disclosure granted otherwise than in consequence of, or under, the Contract;

b. has the right to use or disclose the Information in accordance with other conditions of the Contract; or

c. can show:

(1) that the Information was or has become published or publicly available for use otherwise than in breach of any provision of the Contract or any other agreement between the parties;

(2) that the Information was already known to it (without restrictions on disclosure or use) prior to it receiving it under or in connection with the Contract;

(3) that the Information was received without restriction on further disclosure from a third party who lawfully acquired it and who is under no obligation restricting its disclosure; or

(4) from its records that the same information was derived independently of that received under or in connection with the Contract; provided the relationship to any other Information is not revealed.

6. Neither party shall be in breach of this Condition where it can show that any disclosure of Information was made solely and to the extent necessary to comply with a statutory, judicial or parliamentary obligation. Where such a disclosure is made, the party making the disclosure shall ensure that the recipient of the Information is made aware of and asked to respect its confidentiality. Such disclosure shall in no way diminish the obligations of the parties under this Condition.

7. The Authority may disclose the Information:

a. to any Central Government Body for any proper purpose of the Authority or of the relevant Central Government Body, which shall include disclosure to the Cabinet Office and / or HM Treasury for the purpose of ensuring effective cross-Government procurement processes, including value for money and related purposes. Where such a disclosure is made the Authority shall ensure that the recipient is made aware of its confidentiality;

b. to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;

c. subject to Clause 8 below, to the extent that the Authority (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;

d. subject to Clause 8 below, on a confidential basis to a professional adviser, consultant or other person engaged by any of the entities defined in DEFCON 501 (including benchmarking organisation) for any purpose relating to or connected with this Contract;

e. on a confidential basis for the purpose of the exercise of its rights under the Contract; or

f. on a confidential basis to a proposed body in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under the Contract;

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Authority under this DEFCON.

8. Where the Authority intends to disclose Information to a commercial entity which is not a Central Government Body in accordance with Clauses 7.c or 7.d above, the Authority will endeavour to provide the Contractor with 3 Business Days' notice in advance of such disclosure. In relation to a disclosure of Information made under Clause 7.c above, if reasonably requested by the Contractor within 2 Business Days of such notice being given, where the Authority has not already done so, it will endeavour to procure from the intended recipient of the Information an agreement containing confidentiality terms the same as, or substantially similar to, those placed on the Authority under this DEFCON.

9. Before sharing any Information in accordance with clause 7 above, the Authority may redact the Information. Any decision to redact information made by the Authority shall be final.

10. The Authority shall not be in breach of the Contract where it can show that any disclosure of

Information is made solely and to the extent necessary to comply with the Freedom of Information Act 2000 (“the Act”) or the Environmental Information Regulations 2004 (“the Regulations”). To the extent permitted by the time for compliance under the Act or the Regulations, the Authority shall consult the Contractor where the Authority is considering the disclosure of Information under the Act or the Regulations and, in any event, shall provide prior notification to the Contractor of any decision to disclose the Information. The Contractor acknowledges and accepts that its representations on disclosure during consultation may not be determinative and that the decision whether to disclose Information in order to comply with the Act or the Regulations is a matter in which the Authority shall exercise its own discretion, subject always to the provisions of the Act or the Regulations. For the avoidance of doubt, nothing in this Condition shall affect the Contractor’s rights at law.

11. Nothing in this Condition shall affect the parties' obligations of confidentiality where information is disclosed orally in confidence

ENCLOSURE 4 TO
SAL 713539451 - HMS CASSANDRA Wreck Survey
DATED 29/01/2025

DEFCON 76 (Edn 11/22) **Contractors Personnel at Government Establishments**

Definitions

1. Reference in this Condition to:

a. 'Government Establishment' or 'site' shall be deemed to include any of His Majesty's Ships or Vessels and Service Stations;

b. 'Officer in Charge' shall be deemed to include Officers Commanding Service Stations, Ships' Masters or Senior Officers, and Heads of Government Establishments; and

c. 'Contractor's Representative(s)' shall be deemed to include the Contractor's employees, agents and subcontractors.

General

2. The following general provisions apply:

a. The Officer in Charge shall provide such available administrative and technical facilities for the Contractor's Representatives employed at Government Establishments for the purpose of the Contract as may be necessary for the effective and economical discharge of work under the Contract. These facilities will be provided free of charge unless otherwise stated in the Contract. The status to be accorded to the Contractor's Representatives for messing purposes will be at the discretion of the Officer in Charge.

b. Any land or premises (including temporary buildings) made available to the Contractor by the Authority in connection with the Contract shall be made available to the Contractor free of charge, unless otherwise stated in the Contract, and shall be used by the Contractor solely for the purposes of performing the Contract. The Contractor shall have the use of such land or premises as licensee and shall vacate the same upon completion of the Contract. Any utilities required by the Contractor shall be subject to the charges set out in the Contract.

c. The Contractor shall have no claim against the Authority for any additional cost or delay occasioned by the closure for holidays of Government Establishments, where this is made known to them prior to entering into the Contract.

Liability In Respect Of Damage To Government Property

3. Without prejudice to the provisions of DEFCON 611 (Issued Property) and of DEFCON 612 (Loss of or Damage to the Articles), where those conditions form part of the Contract, the Contractor shall, except as otherwise provided for in the Contract, make good or, at the option of the Authority, pay compensation for all damage occurring to any Government Property, which includes land or buildings, occasioned by the Contractor, or by any of their Representatives, arising from the Contractor's or their Representatives' presence on a Government Establishment in connection with the Contract, provided that this Condition shall not apply to the extent that the Contractor is able to show that any such damage was not caused or contributed to by any circumstances within the Contractor's or their Representatives' reasonable control.

4. The total liability of the Contractor under Clause 3 herein shall be subject to any limitation specified in the Contract.

Contractor's Property

5. All property of the Contractor and their Representatives shall be at the risk of the Contractor whilst it is on any Government Establishment, and the Authority shall accept no liability for any loss or damage howsoever occurring thereto or caused thereby, except as follows:

a. where any such loss or damage was caused or contributed to by any act, neglect or default of any Government Servant, agent or contractor then the Authority shall accept liability therefor to the extent to which such loss or damage is so caused or contributed to as aforesaid; and

b. where any property of the Contractor has been taken on charge by the Officer in Charge, and a proper receipt has been given therefor, then the Authority shall be liable for any loss or damage occurring to that property while held on such charge as aforesaid.

Contractor's Representatives

6. The Contractor shall submit in writing to the Authority for approval, initially and as necessary from time to time, a list of their Representatives who may need to enter a Government Establishment for the purpose of, or in connection with, work under the Contract, giving such particulars as the Authority may require, including full details of birthplace and parentage of any such Representative who:

a. was not born in the United Kingdom; or

b. if they were born in the United Kingdom, were born of parents either or both of whom were not born in the United Kingdom.

7. The Authority shall issue passes for those Representatives who are approved by it in accordance with Clause 6 herein for admission to a Government Establishment and a Representative shall not be admitted unless in possession of such a pass. Passes shall remain the property of the Authority and shall be surrendered on demand or on completion of the work.

8. Notwithstanding the provisions of Clauses 6 and 7 hereof if, in the opinion of the Authority, any Representative of the Contractor shall misconduct themselves, or it shall not be in the public interest for any person to be employed or engaged by the Contractor, the Contractor shall remove such person without delay on being required to do so and shall cause the work to be performed by such other person as may be necessary.

9. The decision of the Authority upon any matter arising under Clauses 6 to 8 inclusive shall be final and conclusive.

Observance Of Regulations

10. The following provisions apply:

a. The Contractor shall ensure that their Representatives have the necessary probity (by undertaking the Government's Baseline Personnel Security Standard) and, where applicable, are cleared to the appropriate level of security when employed within the boundaries of a Government Establishment.

b. Where the Contractor requires information on the Government's Baseline Personnel Security Standard (the Standard) or security clearance for their Representatives or is not in possession of the relevant rules, regulations or requires guidance on them, they shall apply in the first instance to the Project

Manager/Equipment Support Manager.

c. On request, the Contractor shall be able to demonstrate to the Authority that the Contractor's processes to assure compliance with the standard have been carried out satisfactorily. Where that assurance is not already in place, the Contractor shall permit the Authority to inspect the processes being applied by the Contractor to comply with the Standard.

d. The Contractor shall comply and shall ensure that their Representatives comply with the rules, regulations and requirements that are in force whilst at that Establishment which shall be provided by the Authority on request.

e. When on board ship, compliance with the rules, regulations, and requirements shall be in accordance with the Ship's Regulations as interpreted by the Officer in Charge. Details of those rules, regulations and requirements shall be provided on request by the Officer in Charge.

Transport Overseas

11. Where the Contractor's Representatives are required by the Contract to join or visit a Government Establishment overseas, transport between the United Kingdom and the place of duty (but excluding transport within the United Kingdom) shall be provided free of charge by the Authority whenever possible, normally by Royal Air Force or by MOD chartered aircraft. The Contractor shall make such arrangements through the Project Manager/Equipment Support Manager named for this purpose in the Contract. When such transport is not available within a reasonable time, or in circumstances where the Contractor wishes their Representatives to accompany materiel for installation which they are to arrange to be delivered, the Contractor shall make their own transport arrangements. The Authority shall reimburse the Contractor's costs for such transport of their Representatives on presentation of evidence supporting the use of alternative transport and of the costs involved. Transport of the Contractor's Representatives locally overseas which is necessary for the purposes of the Contract shall be provided wherever possible by the Authority and, where so provided, will be free of charge.

Medical Treatment Overseas

12. Out-patient medical treatment given to the Contractor's Representatives by a Service Medical Officer or other Government Medical Officer at a Government Establishment overseas shall be free of charge. Treatment in a Service hospital or medical centre, dental treatment, the provision of dentures or spectacles, conveyance to and from a hospital, medical centre or surgery not within the Establishment, and transportation of the Contractor's Representatives back to the United Kingdom, or elsewhere, for medical reasons, shall be charged to the Contractor at the appropriate local rate.

Injuries, Disease and Dangerous Occurrences

13. The Contractor shall report any injury, disease or dangerous occurrence at any Government Establishment arising out of the performance of this Contract, which is required to be reported under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) to the Officer in Charge of the relevant Government Establishment. This would be in addition to any report, which the Contractor may be required to submit under RIDDOR to the relevant enforcing authority (e.g. Health and Safety Executive or Local Authority).

Dependants of Contractor's Representatives

14. No assistance from public funds, and no messing facilities, accommodation or transport overseas shall be provided for dependants or members of the families of the Contractor's Representatives. Medical or

necessary dental treatment may, however, be provided for dependants or members of families on repayment at current MOD rates.

Provision of Funds Overseas

15. The Contractor shall, wherever possible, arrange for funds to be provided to their Representatives overseas through normal banking channels (e.g. by travellers cheques). If banking or other suitable facilities are not available, the Authority shall, upon request by the Contractor and subject to any reasonable limitation required by the Contractor, make arrangements for payments, converted at the prevailing rate of exchange (where applicable), to be made by the Establishment to which the Contractor's Representatives are attached. All such advances made by the Authority shall be recovered from the Contractor.

Health And Safety Hazard Control

16. Where the Contractor enters a Government Establishment for the purpose of performing work under the Contract:

a. The Contractor shall notify the Officer in Charge or the site project liaison officer or overseeing officer nominated in the Contract of:

(1) any health and safety hazards associated with the work to be performed by them or any of their Representatives;

(2) any foreseeable risks to the health and safety of all persons associated with such hazards; and

(3) any precautions to be taken by them as well as any precautions which, in their opinion, ought to be taken by the Authority, in order to control such risks.

b. The Authority shall notify the Contractor of:

(1) any health and safety hazards which may be encountered by the Contractor or any of their Representatives on the Government Establishment;

(2) any foreseeable risks to the health and safety of the Contractor or any of their Representatives, associated with such hazards; and

(3) any precautions to be taken by the Authority as well as any precautions which, in its opinion, ought to be taken by the Contractor, in order to control such risks.

c. The Contractor shall notify their Representatives of and, where appropriate, provide adequate instruction in relation to:

(1) the hazards, risks and precautions notified by them to the Authority under sub-Clause 16.a.;

(2) the hazards, risks and precautions notified by the Authority to the Contractor under sub-Clause 16.b.; and

(3) the precautions which, in their opinion, ought to be taken by their Representatives in order to control those risks.

d. The Contractor shall provide the Officer in Charge or the site project liaison officer or overseeing officer nominated in the Contract with:

(1) copies of those sections of their own and, where appropriate, their Representatives' Safety Policies which are relevant to the risks notified under sub- Clause 16.a.;

(2) copies of any related risk assessments; and

(3) copies of any notifications and instructions issued by them to their Representatives under sub-Clause 16.c.

e. The Authority shall provide the Contractor with:

(1) copies of those sections of its own Safety Policies which are relevant to the risks notified under sub-Clause 16.b.;

(2) copies of any related risk assessments; and

(3) copies of any notifications and instructions issued by it to its employees similar to those called for from the Contractor under sub-Clause 16.c.