Issued: Jan 16
Review Period: 12 Months
Next Review: Jan 17

MARITIME INFORMATION SUPERIORITY DIVISION
TERMS OF REFERENCE

Post Title	CDOC ET WATCH 5
HRMS, JPA or Magellan Number	2083882
Rank/Grade	AB(CIS) - FTRS
Location	D Leg MCSU Room D13

Role and Responsibilities (these boxes will be cut/pasted into the JPA 'Responsibilities' field and will appear on page one of your OJAR/SJAR.:

Watch keep as part of a 5 watch system 24/7 365 in CDOC Watch 5
Populate Remedy in support of Incident and Change Management Processes
Management of on-going Remedy cases including closing Remedy Calls
Minor Fault Diagnosis to provide 1st line fix to end users whenever possible
Undertake Remedy training as required when new processes are adopted
Defensive monitoring of front line IS Systems
Defensive Cyber monitoring of NSoIT(D) Red, Black and Blue

PREAMBLE

1. The Royal Navy Headquarters generates and develops maritime forces. ACOS IS is responsible for planning and implementing the through life Development and Integration of the Fleet's C5ISR capability across all lines of development and managing the information Defence Line of Development across the Fleet. ACOS IS is also deputy Command Information Officer for the RN (DCIO RN). Underneath ACOS IS sits the Delivery Team that is responsible for the overall Delivery of Maritime Information Superiority Capability.

ACCOUNTABILITY

2. CDOC ET Watch 5 is accountable to the CDOC Watch 5 Team Leader.

AUTHORITY

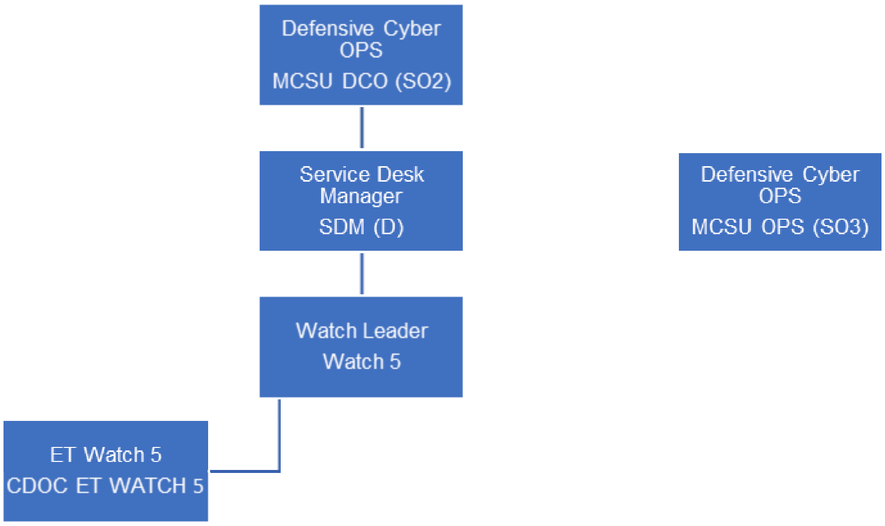
3. The role of CDOC ET Watch 5 has the following authority:

a. CDOC ET Watch 5 is authorised to liaise with all MOD authorities, other National, NATO, Allied military commanders and other Governmental departments to achieve his primary purpose.

b. Communication. CDOC ET Watch 5 is authorised to correspond on behalf of NAVY COMMAND HQ and MCSU in the discharge of their MCSU responsibilities.

ORGANISATION

4. Organisation Diagram:



ROLE

5. To shift-work as part of the MCSU Cyber Defence Operating Centre (CDOC) 24/7 working routine, in its role as the central, single point of contact between MCSU resolver teams, external service providers and the operational users/customers. This role facilitates the unit's ability to meet COMOPS priorities, the RN Plan and endorsed ACOS IW requirements in support of Navy Board Standing Objectives. The CDOC will operate 24/7 365 with 5 watches to allow for watchkeepers leave, annual leave and training. MCSU will take on Level 3 support and Defensive Cyber Monitoring for New Style of IT (Deployed) (NSoIT(D)) Red, Black and Blue.

PRIMARY OBJECTIVES

6. The objectives for the role of CDOC ET Watch 5 are:

a. Take and log calls using Remedy support tools into the MCSU service Desk via email and telephone.

b. Provide 1st line fix support to customers using available technical information on services supported by MCSU.

c. Produce reports using Remedy and Business Objects for use by MCSU CDOC Watch Leader.

d. Carryout out Defensive Cyber Monitoring for MCSU supported IS Systems

e. Carryout out Defensive Cyber Monitoring on NSoIT(D).

COMPETENCES

7. Training on the Remedy Service Management and Business Objects tool sets is performed in-house and once the post holder has joined the unit. In general, the post holder is to have:

a. Rank/Grade: Able Rating

b. Branch/Specialisation/Sub-specialisation: CIS

c. Competencies: Preferably (all though not essential) the post holder has previous sea experience in LPH/LPD/FF/DD platforms. A good systems knowledge is beneficial but not essential.

d. Security Clearance levels: Developed Vetting is not essential but may be beneficial if already held. The post holder is to have current SC security clearance.

7. In addition, this post requires the following specific competencies:

Competence	Course Ref	Skill Level		
		Basic	Int	Adv
Security Cleared		x		
Cat B Driving Licence		x		
Remedy Service Management Toolset	At unit		x	
MODNET - DII(S) – User			x	
MS Office			x	
Word User			x	
Excel User			x	
Annual Security Brief (NCT 3)		x		
DIMP			x	
NSoIT(D)	To be published	x		
Cyber Foundation Pathway (CFP)	Modules 0-4		x	

8. NSoIT(D) and Cyber Foundation Pathway (CFP) courses will be conducted once available, currently planned for Q2 2020. CFP preparation courses can be conducted on the Defence Learning Environment (DLE) with modules 1-4 taking place at the Defence Academy Shrivenham.

9. Further training may be available in ITIL, SPLUNK, DCC and DCC Applications and will depend upon NSoIT future rollout programme and its associated applications.