**Contract REQ 61758453 - £0.01p**

**REQUEST FOR INFORMATION: DRAFT User Requirements Document (URD) for the Commercial Analysis of Safety Critical Data Held in Navy Lessons Information Management System (NLIMS)**

**Issue**

1. The current Navy Lessons Information Management System (NLIMS) is due to be retired, either through development of a new NLIMS database in Foundry or adoption of a derivative of the Defence Unified Reporting and Learning System (DURALS). NLIMS holds safety critical data in approx. 37,000 records. These records will not be transferred upon retirement and therefore Navy Command will not have the ability to learn from these legacy records, which is compounded by the absence of in-house skills, capacity and software tools to analyse these records in a meaningful way for organisational learning. Therefore, it is essential the Navy Safety Centre (NSC) procures commercial services to analyse NLIMS records to meet 1SL’s legal and moral duty of care.

**Detail**

2. The NSC would like to conduct a detailed analysis of NLIMS data to maximise organisational learning from existing data. Deliverables:

a. Data analysis of approx. 37,000 NLIMS records against requirements of the Health and Safety Act Work Act 1974 and associated Regulations, such as RIDDOR.

b. An assessment of Navy Command HSEP performance and ability to learn from occurrences.

c. Analysis should also provide analysis of risk exposure in accordance with ISO 31000 and JSP 892[[1]](#footnote-2)

d. Identify causal factors and weight causality using recognise mapping techniques.

e. Propose improvements to the reporting, analysis and exploitation of safety lessons using advanced machine learning/AI techniques.

3. **Deliverables.** The final report would be:

1. Written in MS Word; the format shall be agreed between Supplier and Authority and must be in a logical indexed structure. The Supplier may also wish to provide a verbal brief using MS PowerPoint.
2. Supporting data can be held in MS Excel.
3. The Supplier will use specialist software and analytics tools where necessary.
4. The final report is to be presented in soft copy and presented in-person.

4. **Security Requirements.** There is a need to:

1. Comply with Security Aspects Letter up to UK Security Classification SECRET.
2. Access the NLIMS database records are classified upto UK OFFICIAL-SENSITIVE.
3. The overall combined risk picture report shall be classified UK SECRET.
4. NLIMS data can be transferred to the Supplier for analysis, but specific permission is mandatory.
5. Data is not to be retained or used beyond contract duration.
6. Comply with DEFCON 532B and associated DEFFORM. Suppliers will be handling personal information for which GDPR applies.
7. Hold Cyber Essentials Plus in accordance with Cyber Risk Assessment.
8. Hold List X Status should the supplier intend to process MOD data outside MOD premises. More information can be found at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/367514/Security_Requirements_for_List_X_Contractors.pdf>
9. Due to immediate processing of OS data, individuals must hold a minimum of Security Check (SC) security clearance from contract award.

5. **Support**. The NSC will provide the following support to the successful Supplier:

a. Access to relevant NLIMS data. Access to BRd10[[2]](#footnote-3) for a description of Navy Command’s information management system.

b. Access to Subject Matter Experts (SMEs) in Navy Command.

6. **Principles**. The following principles are to be satisfied by the successful bidder(s):

a. **Specialist Expertise & Good Practice**.The successful bidder(s) **must** be an SME and able to draw upon relevant good practice in their analysis and recommendations, providing in-depth and demonstrable knowledge of:

1. Relevant HSEP legislation, policy and guidance applicable to Navy Command[[3]](#footnote-4)[[4]](#footnote-5)[[5]](#footnote-6)[[6]](#footnote-7)[[7]](#footnote-8)
2. Systemic analysis of human factors
3. Aggregation and reporting of data to evidence safety learning
4. Systems approach to safety management
5. Causal analysis and risk mapping techniques
6. Exemplar HSEP information management systems, including dashboards
7. Navy Command operations in land, sea and air environments
8. Benchmarking against industry safety performance

b. **Simplicity.** The analysis, report structure and findings should be presented in plain English and digestible to a non-technical audience.Recommendations, where applicable, shall be specific, measurable, achievable, realistic and with suggested time scales.

c. **Future Work**. Navy Command is a high performance / high reliability organisation that demands continual improvement. Whilst this Review is focused on providing independent analysis of NLIMS, the findings will also be used to inform and help de-risk future work by Navy Command to digitise all HSEP related data and deliver an enduring content analytics capability.

**END**

1. ISO 31000 – International Standard for Risk Management, JSP 892 – MOD Risk Management Policy. [↑](#footnote-ref-2)
2. Navy Command Safety and Environmental Management System. [↑](#footnote-ref-3)
3. BRd 10 - Navy Command Safety and Environmental Management System. [↑](#footnote-ref-4)
4. JSP 815 – Defence SMS Framework. [↑](#footnote-ref-5)
5. UK Health and Safety At Work Act, 1974 and Management of Health and Safety at Work Regulations, 1999 (Amended 2003). [↑](#footnote-ref-6)
6. Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR). [↑](#footnote-ref-7)
7. JSP 375 – Management of Health and Safety in Defence. [↑](#footnote-ref-8)