Annex C - Security Considerations

This document accompanies the Invitation to Tender (ITT) for an electronic Safeguards Information Management and Reporting System (SIMRS). It details additional information regarding the security aspects of the SIMRS.

Sensitive Nuclear Information (SNI) is information relating to activities carried out on, or in relation to, civil nuclear premises which needs to be protected in the interests of national security. The Nuclear Industries Security Regulations (NISR) 2003 requires those who operate within the civil nuclear industry to protect SNI in an appropriate manner. The SIMRS will process SNI classified at up to and including OFFICIAL–SENSITIVE.

1. SNI is defined in the Anti-terrorism, Crime and Security Act (ATCSA) 2001 (as amended), as including:

    - Information relating to activities carried out on or in relation to nuclear sites or other nuclear premises which appears to the Secretary of State to be information which needs to be protected in the interests of national security.

2. This definition is further amplified in NISR 2003 and The Energy Act (TEA) 2013. ATCSA and TEA share the same basic definition of SNI. NISR defines SNI by reference to ATCSA but adds that SNI includes information that needs protective marking under the ONR Classification Policy.

3. Whilst not taking precedent over the legal definitions within the statute above, a working definition of SNI can be described as information:

    - Relating to activities carried out on or in relation to civil nuclear premises; and
    - Of value to an adversary planning a hostile act.

4. The Government Security Classifications (GSC) policy details that there is no expectation that routine OFFICIAL information will be marked. SNI is included in the official sensitive subset of OFFICIAL information. This subset covers information that could have more damaging consequences if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but it attracts additional measures to reinforce the 'need to know'. Therefore, OFFICIAL-SENSITIVE assets that contain SNI should be conspicuously marked OFFICIAL-SENSITIVE:SNI (O-S:SNI).

5. The supplier should ensure that the SIMRS is secure and resilient to cyber threats by integrating security into design, implementation, operation and

maintenance activities. The security outcome and response strategy that the Cyber Protection System for the SIMRS should achieve is detailed in ONR Security Assessment Principles[1]; and Technical Assessment Guide (TAG) 7.3 – Protection of Nuclear Technology and Operations[2].

6. In addition, the following baseline controls in relation to how O-S:SNI is protected must be applied to the SIMRS:

a. Electronic Information at Rest	- Electronic Information must be protected at rest by default. This may be by appropriate physical protection (such as data at rest in an accredited data centre); or must involve Foundation Grade[3] data at rest encryption when physical control isn't guaranteed (such as on a laptop).
b. Electronic Information in Transit	- Information in transit between trusted organisations will be via accredited shared infrastructure (such as Public Services Network (PSN)). - Where it must be shared with external partners (e.g. emailed over the Internet), it must be protected using Foundation Grade encryption.
c. ICT Systems (stand-alone, LAN or WAN) and Services	- All communications and IT systems used for processing and accessing O-S:SNI information must be secured in accordance with guidance in ONR TAG 7.3.

[1] http://www.onr.org.uk/syaps/
[2] http://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-7.3.pdf
[3] If a National Cyber Security Centre, Commercial Product Assurance approved Foundation Grade Encryption product is not available, or its use is not practicable, the suppler may make a risk-based decision to use an equivalent assured product.