Ministry of Defence

Industry Security Notice

Number 2021/03

Subject: **Compliance with Cyber Security Requirements from Other Nations (Amended)**

Introduction

1. The UK Defence Supply Base (DSB) is required to comply with the Information and Cyber Security requirements of the UK Ministry of Defence (MOD).

Issue

2. This ISN provides interim instructions for the DSB as to how to address contractual requirements, in order to:

a. assess or certify compliance with the Information and Cyber Security requirements of other nations (such as those set out in the US Defense Federal Acquisition Regulation Supplement (DFARS) / Cybersecurity Maturity Model Certification (CMMC) requirements); and

b. provide representatives of other nations with access to information or equipment on DSB information systems and IT networks, in order to investigate cyber security incidents.

Status

3. This ISN 2021/03 replaces ISN 2018/04 (Interpretation of US DFARS Clauses in relation to CDI and Cyber Reporting).

Scope

4. This ISN covers information systems and IT networks used by the DSB that are either:

   a. accredited by UK MOD;

   b. used for UK MOD contracts/programmes/technology; or

   c. where UK MOD acts as the Designated Security Authority (DSA) on behalf of a partner nation (i.e. the UK is responsible for protecting Foreign Government Classified information).

5. Where DSB activity does not relate to UK MOD, is not conducted on UK MOD accredited networks, or UK MOD is not the DSA, then advice on compliance with Information and Cyber Security requirements for other nations should be sought directly from the relevant Lead Government Department[1] and/or National Technical Authority[2] , to the extent that the DSB information system or network is used in relation to other activity for UK government.

Background

6. Where the DSB is providing activities, programmes or capability to UK MOD, a potential conflict of interest may arise in instances where the DSB may also be required to comply with the information and cyber security requirements imposed on them by foreign parties (in particular Governments, and their associated Prime Contractors).

7. Additionally, the UK government has sovereignty concerns where any information systems, networks or assets in use by DSB for delivering activities, programmes or capability to UK MOD are subject to access by foreign nations.

8. To address these concerns UK MOD are engaged in formal discussions in various forums, including with Five Eyes (FVEY) partners. The aim of these discussions is to investigate mutual recognition and reciprocity so as to reduce and/or eliminate any duplication of effort for Defence and the DSB in achieving and proving assurance of the Supply Chain Cyber Security posture. This includes addressing particular, current, concerns specific to the USA (new and emergent DFARS requirements, including CMMC[3]), which also impinge on other partners nations, as well as recognition of international and local standards for both Official and Industrial Security.

9. UK MOD are also engaged with colleagues across UK Government on all aspects of Cyber Security of the Supply Chain, and remains committed to activity that increases the Cyber Security of the Supply Chain, be it domestic or international.

10. UK MOD continues to work with the DSB in developing security measures, with formal engagement through various channels including, Liaison Group on Defence Industrial

[1] Which, dependant on context, is likely to be BEIS, DCMS, DIT, or FCDO.

[2] Which, dependent on context, will be either CPNI, NCSC, or UK NACE.

[3] Link to information on CMMC.

Security (LGDIS) / DISA (formerly Defence Industrial Security Association), Team Defence Information (TD-Info) and the Defence Cyber Protection Partnership (DCPP).

Action by Industry

11. Until the discussions are complete, and further advice is issued, DSB organisations in scope of this ISN are to take the following actions:

a. Notify the originating contracting authority for any new or amended contracts that due to UK Regulations, and in particular this ISN, there may be problems with any contractual requirements originated from other nations which require UK DSB to:

i. provide details, results of assessments, or other compliance information related to IT and cyber security requirements; and/or

ii. conduct assessments of compliance with IT and Cyber Security requirements; and/or

iii. provide representatives of other nations with access to information or equipment on DSB information systems and IT networks in order to investigate cyber security incidents.

b. Notify the Directorate of Cyber Defence & Risk (CyDR) should the requirements of this ISN not be accepted by other nation's contracting authorities as a basis for compensatory contract variation (e.g. removal of the clauses, insertion of narrative language declaring the clauses to be non-applicable / non-operative), so that UK MOD has visibility and can liaise with the relevant parties as necessary.

c. Where the contract brings DSB organisations within scope of the US DFARS Clauses[4] in particular, in addition to the actions above, they should also:

i. emphasise to the US contracting party that discussions between the UK and US Governments are continuing; and

ii. advise the US contracting party to inform the US DOD international Designated Security Authority (DSA), the Defense Technology Security Administration (DTSA) of this situation.

12. Further advice will be issued on conclusion of the discussions at Government level.

[4] USFR 85-189-61505 Interim Rule "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), which includes the application of Cybersecurity Maturity Model Certification (CMMC) encompassing:

- DFARS Clause 252.204-7020: provision of access to contractor facilities, systems, and personnel from US nationals (contractors or government); and
- DFARS Clause 252.204-7021: invoking of a new approach, "CMMC".

Validity / Expiry Date

13. This ISN will expire when superseded or withdrawn.

MOD Point of Contact Details

14. The point of contact in respect of this ISN is:

Info & Info-Cyber Policy Team
Directorate of Cyber Defence & Risk (CyDR)
Ministry of Defence

email: UKStratComDD-CyDR-InfoCyPol@mod.gov.uk (Multiuser).