Ministry
of Defence

Industry Security Notice

Number 2023/11

Subject: **REQUIREMENT FOR DEFENCE CONTRACTORS TO REPORT ALL SECURITY INCIDENTS AFFECTING DEFENCE RELATED CLASSIFIED MATERIAL TO THE UK MOD.**

Introduction

1. The timely and comprehensive reporting, investigation and remediation of security incidents underpins the assurance of Defence Related Classified Material held both internally and across the Defence Industrial Base. This Industry Security Notice (ISN) replaces ISN 2023/05 for the purpose of updating the Defence Industry WARP contact details. Please note only the telephone number has changed.

2. For the purposes of this ISN, the term Defence Contractors includes companies that have a contractual relationship with the UK MOD, together with their subcontractors, or companies that hold Defence related classified material that has been given a security classification by the UK MOD.

3. For the purposes of this ISN, the term Defence related classified material covers MOD Identifiable Information (MODII) and 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 Contractors which are owned by a third party e.g. NATO or another country which the MOD is responsible for.

4. If a Defence Contractor believes that compliance with the requirements of this ISN will have a material and unavoidable implication on the costs incurred in delivering the product of services under a MOD contract, the Defence Contractor may seek an adjustment to the Contract Price in accordance with DEFCON 620 or any agreed alternative change control procedure.

Issue

5. The purpose of this ISN is to inform Defence Contractors that all security incidents (as defined in paragraph 9 of this ISN) are to be reported to the MOD Defence Industry, Warning Advice and Reporting Point (WARP) within the incident reporting timescales specified in paragraph 18 of this ISN.

Action by Defence Contractors and the MOD Defence Industry WARP

6. The following paragraphs explain the roles of Defence Contractors and the MOD Defence Industry WARP in the resolution of security incidents occurring in industry:

7. **Defence Contractors.** Each Defence Contractor shall maintain an effective internal security reporting system to assist in both the reporting and mitigation of impacts to Defence. Assurance of Defence related classified material under their responsibility shall be achieved by:

a. Compliance with current HMG and UK MOD data handling and storing procedures.

b. Compliance with the terms in defence contracts in respect of disclosure of information and security measures.

c. Co-operation with UK MOD security processes, assurance programmes and security investigations.

d. Engagement in associated security process reviews and improvement initiatives.

e. Proactive engagement and communication with the MOD Defence Industry WARP where the Defence Contractor has identified a previously unmanaged incident, so that risks to information, assets, platforms, systems and personnel can be identified at the earliest opportunity.

f. The prompt reporting of all Cyber, Physical, Personnel and Technical security incidents involving Defence related classified material to the MOD Defence Industry WARP.

8. **MOD Defence Industry WARP.** The MOD Defence Industry WARP is responsible for co-ordinating all incidents reported by Defence Contractors and for engagement with the appropriate Contracting Authority, Subject Matter Experts (SME's), Other Government Department's (OGD's) and law enforcement agencies if necessary. In undertaking this responsibility, it is essential that Defence Contractors report **all** security incidents promptly (further information provided in paragraph 18).

Security incidents

9. The MOD defines a security incident as any circumstance that results in Defence related classified material being damaged, compromised, lost or disclosed to unauthorised persons due to a failure of policy, existing security measures or controls, or something that requires an action/response following a direct threat or individual action. These could be accidental or deliberate acts by those internal or external to the Defence Contractor's organisation. Furthermore, any suspicious activity related to personnel or physical security of assets or MOD operations must also be reported.

10. Security Incidents are categorised under four general domains:

a. **Cyber**; includes all forms of cyber-attacks, malicious software, phishing (if acted upon), ransomware, denial of service, etc.

b. **Physical**; incidents affecting or compromising physical assets or security of a site, building or sensitive area. For example, this includes loss or compromise of hard copy classified documents or Defence equipment.

c. **Personnel**; incidents concerning the integrity of the security vetting regime, misuse of UKSV sponsor account/s, misuse or fraudulent use of access control passes or ID cards. Unsolicited or suspicious approaches either online or in person especially by individuals from countries considered hostile to the UK and potential insider threats where such threats involve Defence interests.

d. **Technical**; incidents concerning the compromise of Defence related classified material by means of eavesdropping or similar technical exploits.

11. It should be noted that classified assets or information that cannot be accounted for are to be considered compromised until it is confirmed otherwise. Therefore, Defence Contractors shall contact the Defence Industry WARP should they be unable to account for any such material.

Incidents involving internationally classified Defence material

12. All actual or suspected incidents of loss, compromise or unaccountability of internationally classified defence material are to be reported to the Defence Industry WARP. Where necessary, MOD will then coordinate upward reporting to the UK National Security Authority (Cabinet Office).

Dual-reporting obligations

13. Except where required by law, the Defence Industry WARP is to be the primary reporting point for Defence Contractor security incidents. However, where a Defence Contractor is contractually obliged to report security incidents by a different means, the dual-reporting of incidents may be required to fulfil both obligations. For example, if a Defence Contractor experiences a cyber incident and has engaged with the National Cyber Security Incident (NCSC) they are also expected to report this incident to the Defence Industry WARP.

Initial security incident reporting

14. Defence Contractors with Restricted Lan Interconnect (RLI) connectivity should report incidents at a security classification of OFFICIAL-SENSITIVE to the WARP via the electronic MOD Security Incident Reporting Form (SIRF) at: https://blackthorn.ahe.r.mil.uk/MSIRS/

15. Where RLI-connected companies are currently unable to connect to the SIRF, the initial report should still be submitted via RLI email in the format shown at Annex A. Defence Industry WARP staff will then raise the SIRF on behalf of the Defence Contractor and provide them with the relevant reference numbers.

16. For Defence Contractors that do not have RLI connectivity, incidents should be reported by telephone (up to OFFICIAL-SENSITIVE, contact details below). The Defence Industry WARP will collate initial details regarding the incident in the format listed at Annex A. If information regarding the incident is not available, this should not delay the initial report. Alternatively, incidents can be reported using a corporate IT providing the system is accredited and the email is encrypted in accordance with OFFICIAL and OFFICIAL-SENSITIVE Contractual Security Conditions.

17. The Defence Industry WARP will ensure the confidentiality and integrity of all Defence Contractor information provided. All incident data provided is stored securely on the Defence Incident Management Database. All data is processed, handled, and stored in compliance with the Data Protection Act 2018.

Incident reporting timescales

18. Initial incident reporting to the Defence Industry WARP is determined by the severity and impact of the incident.

INCIDENT CATEGORY	IMPACT/SEVERITY	MOD/NATO/EU/ESA MATERIAL INVOLVED	INITIAL REPORTING TIMESCALE
RED (P1)*	CRITICAL/SEVERE	Where there is a medium or high risk of compromise (i.e. the information or asset is outside of an access controlled area, in the public domain or likely in the hands of a malicious actor) to TOP SECRET, STRAP, SAP, ATOMIC.	IMMEDIATE
AMBER (P2)	SERIOUS	SECRET, INTERNATIONAL CONFIDENTIAL, NNPPI, PSA or a low risk of compromise (i.e. a breach or reportable incident is identified but the information or asset has remained in an access controlled area with some controls in place) to TOP SECRET, STRAP, SAP, ATOMIC. Personal data breaches impacting MOD personnel. Bulk quantities of data classified as OS, OS(P), OS(C), INTERNATIONAL RESTRICTED.	NLT 24HRS
YELLOW (P3)	MODERATE	OS, OS(P),OS(C), INTERNATIONAL RESTRICTED.	NLT 72 HRS
GREEN (P4)	LOW	OFFICIAL & LOW-LEVEL BREACHES	NLT 5 WORKING DAYS

**Indicative corresponding incident categories in brackets.*

If the incident relates to a Cyber incident, please report in accordance with DEFCON 658.

For further information on the categorisation of an incident please speak to your Security Controller or Defence Industry WARP.

Acknowledgement of report

19. Upon receipt of the incident notification, the Defence Industry WARP will contact the reporter to address any further information requirements to support an accurate assessment of risk to Defence.

Updating the WARP on progress of investigations

20. Following the initial incident report, the MOD appreciates that investigations, especially into technical or complex issues, may take time to conclude. However, it is important that the Defence Industry WARP is kept appraised of the progress of investigations, particularly those which are assessed as CRITICAL/SEVERE and SERIOUS**.**

The Defence Industry WARP will set individual timeframes for Defence Contractors on how frequent they should be updated on the status of the investigation in line with the severity of the incident.

Final reports

21. Incidents categorised as CRITICAL/SEVERE, or SERIOUS require a Final Security Incident Report to be completed in the format shown at Annex B. The Defence Industry WARP will provide tailored guidance on the specific information required by Defence Contractors to compile the report. Once MOD is satisfied that root causes have been identified, risks mitigated and remediation implemented, the Defence Industry WARP will notify the Defence Contractor of the incident's closure.

22. Defence Contractors are required to provide the Defence Industry WARP with details of the individual(s) which were found to have been responsible/culpable for the security breach or incident concerning Defence Related Classified Material. The full name of the individual, their DOB and place of birth is required for individuals which hold a UK National Security Vetting clearance or BPSS.

ISN Validity / Expiry Date:

23. This notice is valid with immediate effect and remains so until further notice.

Point of contact:

24. The MOD Defence Industry WARP contact details are:

Email:	DefenceWARP@mod.gov.uk
RLI Email:	Defence WARP

Telephone (Office hours): 03001 583 640
Defence WARP Out of Hours Duty Officer: 07977807180

Mail: Defence Industry WARP, DE&S PSyA Office, MOD Abbey Wood, NH2 Poplar -1 #2004,Bristol, BS34 8JH.

Annexes:

A. MOD Defence Industry WARP Initial Security Incident Report Template

B. MOD Defence Industry WARP Final Security Incident Report Template

MOD DEFENCE INDUSTRY WARP INITIAL SECURITY INCIDENT REPORT TEMPLATE

Date of report:

Company security incident number:

Associated crime reference numbers (if applicable):

Originator details

1. Originator's title, name, role, company, address, telephone number, Email Address, Contracting Authority.

Incident Detail

2. **WHAT**

   a. Incident type (Cyber, Personnel, Physical, Technical):

   b. What has happened (e.g. Breach, Loss, Compromise, Theft, Hostile Reconnaissance, Damage, Cyber Attack, Phishing Campaign etc):

   c. Level of compromise (e.g. internal, external, public domain etc):

   d. Type, classification, and quantity of material / systems / assets involved:

   e. Detail of any affected MOD codewords or designators if known.

3. **WHEN**

   a. Date, time, and duration of the incident:

   b. Date, time, and duration of detection:

4. **WHERE**

   a. Location of incident:

   b. Location of detection:

5. **HOW**

   a. The means by which the incident occurred.

   b. The means by which the incident was detected

6. **WHY**

   a. Likely causes of the incident (may not be clear initially).

7. **WHO**

   a. Current assessment of likely culpable company parties (individual/s and/or group/s, including their employer/s):

   b. Contracting Authorities (MOD or GC) affected by the incident:

c. Information Asset Owners affected:

d. Any other impacted parties:

8. **IMPACT**

a. Assessment of impact to the reporting company, Defence, and/or, the MOD:

b. Connectivity / impact to:

(1) MOD Core Networks:

(2) MOD Accredited systems or networks:

c. Impact to MOD Personally Identifiable Information and numbers affected:

d. Wider context:

e. Likelihood of media interest:

f. Likelihood of international or parliamentary interest:

g. Impact to NATO, EU, or European Space Agency (ESA) material:

h. Connection or impact to any FSC facilities:

9. **INITIAL INCIDENT RESPONSE**

a. Initial actions by company/s:

b. Internal or outsourced Cyber Incident Response Team deployment:

c. Steps already taken to mitigate the incident:

d. Steps already taken to remediate the incident:

10. **COMMUNICATIONS**

a. Internal communications:

b. External stakeholder / company / MOD engagement:

c. Law Enforcement / NCSC / CPNI / HMG engagement:

d. Reporting in accordance with GDPR / DPA 18:

e. Media engagement:

11. **PLANS**

a. Planned activities, mitigation, remediation:

b. Actions or assistance requested of the MOD:

c. Media strategy:

d. Means / date of next planned update to the MOD:

{Signature Block}

MOD DEFENCE INDUSTRY WARP FINAL SECURITY INCIDENT REPORT TEMPLATE

Date:

Incident reference number (assigned by the WARP):

Title:

1. **Executive Summary.**

   a. Bullet points briefly outlining conclusions.

   b. Include category of breach.

   c. Bullet points outlining recommendations.

2. **Background**. Provide brief details of circumstances leading to investigation. Provide information of any person found culpable:

   a. Full name, service/staff number, date and place of birth, nationality,

   b. Current role/post,

   c. Frequency of access to classified information (e.g., has regular access to SECRET),

   d. National Security Vetting clearance type and expiry date.

3. **Damage Assessment.** A brief summary of any damage assessment (including mitigating factors following implementation of counter compromise action) should be outlined here and the full damage assessment included as an Annex.

4. **Investigation**. Provide overview of lines of enquiry followed. This should not be a chronological list of events but should focus on what evidence was gathered, highlighting key points of evidence and any issues which prevented any specific lines of enquiry being completed.

5. **Conclusions & Lessons Identified.** It is concluded that: (conclusions should be reached on the balance of probability based on the evidence gathered during the investigation. The conclusions should include any areas where there is still a degree of ambiguity).

a. The security breach was graded as Minor/Serious/Gross (MANDATORY requirement).

b. Root causes of the incident including non-adherence to MOD policy / procedures.

6. **Remediation.** Remediation implemented by the company in response to the incident / breach including:

a. Requirements for further/outstanding counter compromise action.

b. Changes to policy / local procedures.

c. Enhancements to Protective or Cyber Security posture.

d. Requirement for additional security training/raising of awareness.

e. Administrative / disciplinary / misconduct action.

f. The submission of Aftercare Incident Reports (AIRs). Further information can be found in ISN 22/11 – Ongoing Personnel Security Requirements for Defence Contractors – Aftercare Responsibilities.

{Signature Block}

Annexes:

Copies of Evidence (if required).

Damage Assessment (if required).