Ministry of Defence

Industry Security Notice

Number 2017/01

Subject: MOD ICT Security Accreditation and The Defence Assurance Risk Tool (DART)

Introduction

1. This ISN details security accreditation requirements that shall always be applied for every industry owned Information and Communications Technology (ICT) system that stores, processes or generates MOD data. This ISN is applicable to all companies, contractors and suppliers who process MOD data, it applies more widely than and supersedes List X Notice 44. The Defence Assurance Risk Tool (DART) has been introduced to enable MOD to register, triage and determine approaches to ICT system security accreditation. DART will help provide MOD with a mature understanding of the ICT security risks across the Department and its industry partners through the information input onto DART by companies and organisations.

2. In addition to gaining ICT system security accreditation as detailed in this ISN, the Defence Cyber Protection Partnership (DCPP) Cyber Security Model (CSM) certification is also required if the DCPP CSM is specified in the relevant contract. It is noted that the DCPP CSM requirements are not the subject of this ISN.

Definitions

3. Throughout this document, the term ICT systems means industry owned ICT systems that a company is responsible for, that are either directly owned, leased or provided by a third party as a service and that store, process or generate MOD information. ICT Systems include equipment, infrastructure and hosting environments and can include applications as detailed later in this ISN.

4. For the purpose of this document, MOD data and MOD information mean the same thing and MOD data includes all information where MOD has a responsibility for requiring

security of the information (this can include company, Other Government Department (OGD), public sector body, NATO and other country's information).

HMG Requirements

5. The HMG Security Policy Framework (SPF)[1] sets out the Government Policy Priorities including that:

a. All information that HMG deals with has value.

b. All ICT systems that manage government information or that are interconnected to them are assessed to identify technical risks.

c. Proportionate assurance processes will provide confidence that these identified risks are being properly managed.

6. Mandatory security outcomes in HMG SPF require that HMG organisations (and partners handling HMG information) have:

a. Arrangements to determine and satisfy themselves that delivery partners, service providers and third party suppliers apply proper security controls.

b. Mechanisms and trained specialists to analyse threats, vulnerabilities, and potential impacts which are associated with business activities.

c. Risks assessed so that informed, practical and effective business enabling decisions can be made by information risk assessment and risk management specialists.

d. Arrangements to determine and apply risk-informed, cost-effective security controls to mitigate the identified risks within agreed appetites. These arrangements must be used, kept current, and be actively managed.

e. Assurance processes to make sure that mitigations are, and remain, effective.

f. A mature understanding of the security risks throughout the organisation.

7. HMG SPF requires Departments (and partners handling HMG information) to consult the full range of policy, advice and guidance provided by the Cabinet Office, Centre for the Protection of National Infrastructure, National Technical Authority for Information Assurance (CESG) and other sources of good practice to shape their business specific approaches and to deliver these policy priorities and mandatory security outcomes. (This wording from

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

HMG SPF predates the formation of the National Cyber Security Centre (NCSC) who now provide a range of this documentation).

MOD's Approach

8. To comply with HMG SPF, MOD requires companies to review all their ICT systems and either register them onto DART to request ICT security accreditation from MOD or to self-evaluate the ICT systems. The Figure 1 flow chart on page 5 shall be used to determine whether to register each ICT system onto DART or to self-evaluate. Certain applications must also be registered on DART and these are detailed at paragraph 27.

9. Proportionate approaches are used by MOD to meet the policy priorities and mandatory security outcomes detailed in the HMG SPF.

10. MOD's Defence Assurance and Information Security (DAIS) organisation will triage ICT systems and applications registered on DART to determine the appropriate approach for the accreditation of ICT system security. Triage can result in accreditation assessment by DAIS, by MOD major business unit accreditors or, if the security risk is sufficiently low, by self-assessment by companies or organisations. Self-assessment will include companies or organisations providing their security evidence onto DART and DAIS issuing a self-assessment accreditation certificate where the evidence indicates sufficient security. As indicated by Figure 1, risks below these levels will be addressed by company or organisation self-evaluation without registration on DART.

11. For clarity it is noted that the DCPP CSM and Cyber Essentials exist alongside DART and the MOD's accreditation process. The security accreditation requirements in this ISN must always be applied for every ICT system otherwise MOD information shall not be stored, processed or generated on that ICT system. DCPP CSM and Cyber Essentials shall be applied where called up in a contract. Security provided as a result of DCPP CSM and Cyber Essentials will be taken into account during the accreditation and self-evaluation of ICT systems as detailed in this ISN.

12. The CSM also contributes to MOD's understanding of security risk. The MOD objective is to achieve minimal duplication of information and effort for the DART ICT security accreditation and CSM submissions. DCPP CSM is the subject of "Defence Standard 05-138 Cyber Security for Defence Suppliers". Cyber Essentials is the subject of "ISN 2016/01 MOD Implementation of Cyber Essentials Scheme".

Aim

13. The aim of this ISN is to:

a. Notify companies, contractors and suppliers of the requirements for ICT system security accreditation and for the use of DART.

b. Raise awareness of the HMG SPF requirements and adoption of DART within Defence industry.

c. Provide information on the process for registering ICT systems on DART and on ICT system self-assessment and self-evaluation under DAIS oversight.

d. Help ensure security is in place for high risk applications by the registration on DART and accreditation of certain software applications.

Issue

14. In accordance with HMG SPF, all MOD information has value and ICT systems shall not store, process or generate MOD information without proportionate risk assessment and risk management. To help ensure the security of MOD information, companies and organisations must review all their ICT systems and either register them onto DART to request ICT security accreditation or self-evaluate their ICT systems and inform DAIS of the evaluation. Figure 1 on page 5 provides a flow chart to direct this review and help determine the appropriate accreditation approach. Certain applications must also be registered on DART and these are detailed at paragraph 27.

15. DART is supporting the activities that secure MOD information and is helping provide the Department with a mature understanding of ICT security risk. DART provides the ability, through scoring and workflows, to apply greater proportionality, prioritisation and management throughout the accreditation process. By answering a proportionate series of questions about an ICT system and the controls that have been put in place, a company will provide the information necessary for DAIS to determine the level of ICT security risk. The information provided will enable DAIS to determine the appropriate accreditation approach. This may result in self-assessment of ICT security by MOD contractors and suppliers where the risk is sufficiently low.

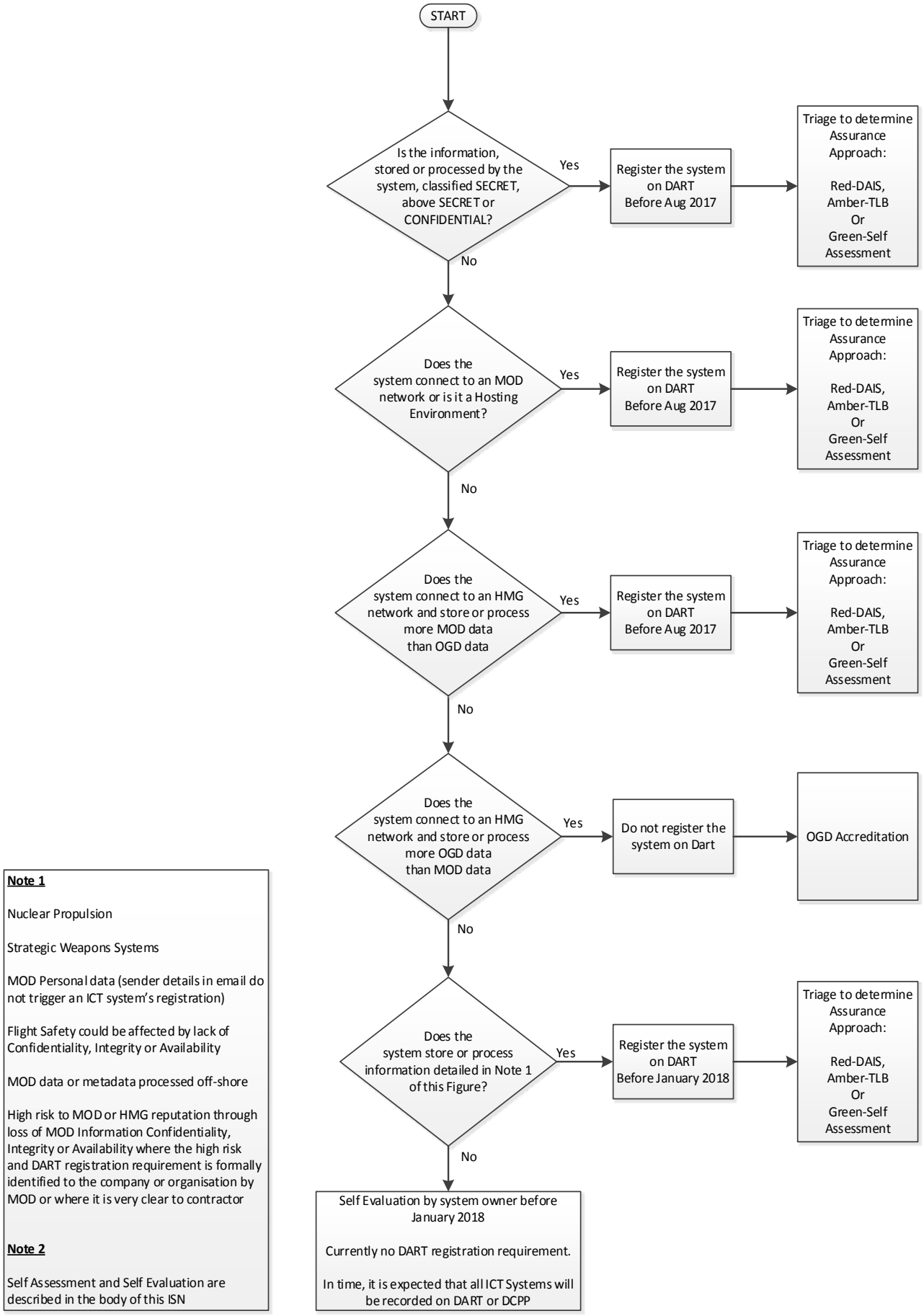

Figure 1 - DART Registration Requirements for Systems Storing or Processing MOD Data

16. Systems that do not require registration on DART, that is the systems that reach the bottom of the flow chart at Figure 1, do require self-evaluation unless the only MOD information they store, process or generate is information that MOD has officially placed in the public domain or is from emails without OFFICIAL-SENSITIVE attachments or content.

17. All ICT system accreditation approaches as well as self-evaluation require the company to comply with the HMG SPF and the related policy and guidance as well as any MOD contract Security Conditions. All self-evaluation and accreditation approaches must comply with the requirements of Third Party data owners such as NATO where their data is being stored, processed or generated. Additional requirements may be specified by MOD contractual governance and these must also be complied with such as the DCPP CSM requirements and as applicable for some contracts, JSP 440 and JSP 604. The required assurance activities shall always be proportionate to the risk.

Self-Assessment and Self-Evaluation

18. Self-assessment and self-evaluation shall be carried out under DAIS oversight and this oversight will normally be achieved through sample based DAIS assurance activities. As a minimum, but in a manner proportionate to the risk, the self-assessment and self-evaluation shall always require the company or organisation to:

a. Assess how loss or compromise of Confidentiality, Integrity or Availability of MOD information stored, processed or generated on each ICT system could occur and how likely that is.

b. Mitigate the risk of loss or compromise by implementing controls to meet the requirements of HMG and MOD policy and guidance including but not limited to the proportionate application of the information available from the following links. If mitigation cannot be achieved, request MOD accept the unknown or insufficiently mitigated risk. Unknown or insufficiently mitigated risk may or may not be acceptable to MOD.

https://www.ncsc.gov.uk/guidance/risk-management-collection

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

https://www.ncsc.gov.uk/guidance

c. For self-assessment but not self-evaluation, check all appropriate controls have been implemented in a proportionate manner by comparison against a standard such as ISO 27002, NIST Special Publication 800-53 or the Baseline Control Set referred to in the Government Security Classification link above. All controls shall be applied or the reason for not using the controls must be documented.

d. Take proportionate steps to assure that the risks are being successfully mitigated on initial assessment and throughout the lifetime of the system and that accepted risk is actively and effectively managed.

e. Audit the self-assessment activities in a proportionate manner.

f. Create evidence in electronic format that verifies all these self-assessment and self-evaluation activities have been successfully carried out.

19. Where the Figure 1 flow chart process led to self-assessment, the electronic format evidence shall be uploaded onto DART where connectivity is available or sent to the DAIS Contact Point whose email and postal address is located at the end of this ISN. Once ICT systems have been registered on DART, triaged and appropriate evidence has been received, DAIS will issue a self-assessment accreditation certificate based on and acknowledging the completed self-assessment.

20. For self-evaluation that was not the result of registration on DART because that was not required after following the Figure 1 flowchart:

a. Companies shall retain the self-evaluation evidence in electronic format and make the evidence available to MOD on request. Unless specifically contracted with MOD to the contrary, to align with the DCPP CSM, the evidence shall be retained for 6 years after termination or expiry of the contract that resulted in MOD information being placed on the ICT system.

b. DAIS shall consider accreditation to have been achieved when the company sends an email to the DAIS Contact Point with a title starting with “Date-Self Evaluation for (ICT system name)”.

(1) The format of the date shall be year month day eg 20170112. An example email title is “20170112-Self Evaluation for xyz system” The email title format is critical to support DAIS automation and enable a large number of companies to send a self-evaluation email successfully.

(2) The email shall be from the company's Security Controller or ICT officer who shall have Board level authority to declare delivery of this accreditation requirement.

(3) The content of the email shall state the company name, a short description of the system, that the self-evaluation has been successfully completed, shall provide contact details and also any DCPP Risk Assessment References from contracts that result in information being stored, processed or generated on the ICT system.

(4) The contact details provided must enable MOD to seek information concerning the ICT system or to arrange an audit of the self-evaluation evidence and these contact details shall be kept up-to-date throughout the life of the ICT system.

(5) MOD shall hold the company responsible for delivering a proportionate and satisfactory self-evaluation.

c. In line with the re-accreditation timescales below, the accreditation shall be valid for three years from the date of the company's self-evaluation completion declaration email unless a change necessitates a new evaluation.

Re-accreditation Timescale

21. Accreditation in the OFFICIAL tier is valid for three years.

22. Accreditation in the SECRET (and CONFIDENTIAL) tier is valid for two years.

23. Accreditation in the Above SECRET tier is valid for one year.

24. A change that would significantly affect ICT system security or a significant security incident shall trigger re-accreditation.

25. In addition to re-accreditation, all ICT systems must be reviewed annually by the company or organisation's Security Controller or ICT officer. This review shall be proportionate, documented and be sufficient to confirm that there has not been a change that would significantly affect ICT system security.

26. These re-accreditation timescales apply irrespective of whether the DAIS accreditor, MOD major business unit accreditor, self-assessment or self-evaluation was the process used.

Application Security and Registration on DART

27. Applications used to store, process, or generate MOD information are considered under four categories, Legacy, Business, System and Corporate. These applications must be registered on DART using the application question set in accordance with the following paragraphs. The accreditor for an ICT system may require additional use of the DART application question set if they have security concerns and deem it proportionate.

Legacy applications

28. Legacy applications are those that are no longer supported by the manufacturer or where a company no longer has the information, skill set or equipment available to maintain the application.

29. Legacy applications shall always be registered on DART.

Business applications

30. Business applications are:

a. All web apps and portal applications where users input information.

b. All bespoke user productivity applications. These include completely bespoke applications and applications with a bespoke front end or user interface such as applies with some databases.

31. Unless the accreditor for the host system has substantial reason to declare otherwise, Business applications must always be registered on DART using the application question set if the application itself, or the ICT system hosting the Business application, is used to store, process or generate the following types of MOD data:

a. MOD Personal data sets totalling 1000 records or more
b. MOD Sensitive Personal data.
c. SECRET or TOP SECRET information.
d. STRAP or Special Access Programme (SAP) information.
e. MOD information (including metadata) stored, processed, or generated off-shore.
f. Nuclear propulsion, strategic weapon systems or ATOMIC information.
g. Information where Flight Safety could be affected by lack of Confidentiality, Integrity or Availability

System applications

32. System applications are those that relate to the ICT system itself not the use the system is put to. Operating systems such as Microsoft Windows, software firewalls and system authentication software are examples and these are assured as part of a system's accreditation.

33. System applications do not need to be registered on DART using the DART application question set unless specifically requested by the accreditor.

Corporate applications

34. Corporate applications such as Commercial Off The Shelf (COTS) word processors and spreadsheets do not require DART registration unless specifically requested by the accreditor. An example where the accreditor might want the application question set used could be for a high risk case such as a lesser known COTS database used for bulk OFFICIAL-SENSITIVE personal data. The host system that corporate applications reside on must have followed Figure 1 and successfully achieved the appropriate accreditation approach. The host ICT system accreditation must also be valid for the type of MOD information stored, processed or generated within each new application installed on the ICT system.

Future aspirations

35. It is an aspiration that each type of corporate and system application a company uses, be registered on DART once for each organisation. The aim is to give MOD sight of the applications used to store, process, transmit or generate MOD information.

ICT System Registration on DART

36. MOD contractors and suppliers with access to the online DART tool must register through that online system where Figure 1 indicates the DART registration requirement. Companies without access to the online tool must use the DART Initial Registration Form (IRF) detailed below in paragraph 44. On receipt of an IRF, DAIS will input onto DART sufficient information to register the ICT system and triage the request. This DAIS registration for companies without access to the current online DART tool will be carried out as a short term temporary measure. DART is being developed to enable all companies to electronically input information. Once this development has occurred and providing the company's ICT system still processes MOD data, companies are required to retrospectively

input any additional information necessary to complete the DART entry themselves when access is provided.

37. ICT systems requiring registration must have their details input onto DART as soon as it becomes known that MOD information will be stored or processed on an unaccredited ICT system, at the time of re-accreditation or in accordance with the dates in Figure 1, whichever is the earlier.

Provision of Evidence to DAIS

38. Appropriate and proportionate evidence must be provided to support accreditation certification and this must include evidence of risk assessment, the application of appropriate and proportionate controls, assurance activities to confirm controls are working and a commitment to maintain the risk assessment, controls and assurance throughout the life of the system. Evidence provided by answering the DART question set does not need to be duplicated in other evidence provided to DAIS as long as the totality of information provided is well structured and cohesive. DAIS will move submitted evidence to appropriate storage to take account of DART aggregation issues.

39. Evidence shall always be provided in electronic format and shall be uploaded onto DART where connectivity is available or sent to the DAIS Contact Point whose email and postal address is located at the end of this ISN. Where an MOD accreditor has been allocated, information sent to the DAIS contact point shall be copied to the accreditor. Evidence can be provided by:

a. Completing the relevant parts of DART's online question set or by completing an IRF and Annex and sending it by email or CD.

b. Uploading evidence onto DART.

c. Providing evidence in electronic format by email or CD.

d. Agreeing an alternate method with DAIS where the evidence is classified SECRET or higher

e. A combination of the above methods.

Maintain a record of MOD information

40. Companies and organisations shall maintain a record of the MOD information stored on every ICT system. As a minimum this must include just sufficient detail that the impact of loss of Confidentiality, Integrity and Availability can be ascertained by MOD and minimised if

the ICT system should be lost or compromised. This information shall be stored in a manner that means it is highly likely to be available if the ICT system it pertains to becomes unavailable.

Accreditation of Sub-contractors

41. As a minimum, the prime contractor shall confirm that their immediate sub-contractors, for each MOD contract, have met the outcomes detailed in this ISN for ICT systems they will use for the contract. The prime contractor shall not provide or enable MOD information to be stored, processed or generated on their sub-contractor's ICT systems until they have confirmed these requirements have been achieved and will be maintained. This process shall be cascaded down the sub-contract chain so for instance, the sub-contractor must confirm the sub-sub-contractor has the met outcomes detailed in this ISN for ICT systems they will use for the contract. Throughout the chain of sub-contractors, MOD information shall not be provided to lower level sub-contractors, to be stored, processed or generated on the sub-contractor's ICT systems, until the contracting company has confirmed these requirements have been achieved and will be maintained by their sub-contractor.

Security Competence

42. Companies and organisations responsible for ICT systems must have access to appropriately competent ICT security expertise to deliver the outcomes detailed in this ISN and to provide accurate evidence and submissions. For smaller systems this does not mean a dedicated ICT security expert is employed full time (at the extreme, for the smallest lowest risk ICT systems it can be just hours per year). Suitably security cleared contractors or a company's permanent staff can supply this expertise if they have an appropriate mix of experience and/or qualifications.

Provision of Policy and Guidance to Companies

43. Access to the policy and guidance, required to enable companies to ensure ICT systems to comply with HMG and MOD requirements, shall be made available by the MOD Project team or Contracting Authority to the prime contractor. The prime contractor shall ensure that policy and guidance is available to their related sub-contract chain.

Completion of DART Submissions

44. Companies must complete the online DART submission or where they do not have access to DART, submit their registration on the latest version of the IRF form, which is available on the DAIS page of the Gov.uk website at: (https://www.gov.uk/government/publications/industry-accreditation-request-form). Information entered onto DART must not exceed OFFICIAL-SENSITIVE. Where the information pertaining to an ICT system exceeds OFFICIAL-SENSITIVE, the system must still be registered on DART using up to and including OFFICIAL-SENSITIVE information with the SECRET or more highly classified information passed through appropriate channels to support the accreditation process.

45. Systems and applications registered on DART must have a unique title related to the capability they provide. For example, 'Oracle Database' would be unacceptable whereas 'The Regiment 1 Supplies Storage Database' or 'Company Name Red Network' would meet the uniqueness requirement. The system or application description recorded in DART must include sufficient detail to provide an overview but must keep within the maximum OFFICIAL-SENSITIVE marking that applies to the DART system.

Development of DART

46. Development of DART will continue, including the addition of modules covering other risk-related activities undertaken by DAIS. Feedback from industry to support the development of DART is welcome and should be forwarded by email to the DAIS contact point.

Action by Industry

47. To follow the requirements of this ISN and apply the process for raising accreditation requests and obtaining accreditation with immediate effect.

Validity / Expiry Date

48. To be reviewed annually in consultation with industry partners.

MOD Point of Contact Details

49. Any queries or issues should be forwarded in writing by email to the DAIS Contact Point: Email: CIO-DSAS-ContactPoint@mod.gov.uk This email should not be used for

OFFICIAL-SENSITIVE unless it has been confirmed that TLS encryption is active between MOD and the company sender/recipient and that the email will land on a system accredited as suitable for OFFICIAL-SENSITIVE caveat information.

Companies who know they have an appropriate connection may send OFFICIAL-SENSITIVE caveat email using: - cio-dsas-contactpoint@diif.r.mil.uk

OFFICIAL-SENSITIVE may also be discussed on 01480 52451 4564 or 01480 446311. Companies connected to the RLI can find further guidance concerning the online operation of DART in the DART User Guide at: (http://defenceintranet.diif.r.mil.uk/libraries/8/Docs2/20140621.10/DART_User_Guide_270614.pdf).

DAIS Contact Point
X007 Bazalgette Pavilion
RAF Wyton
Huntingdon
Cambs, PE28 2EA

7 February 2017