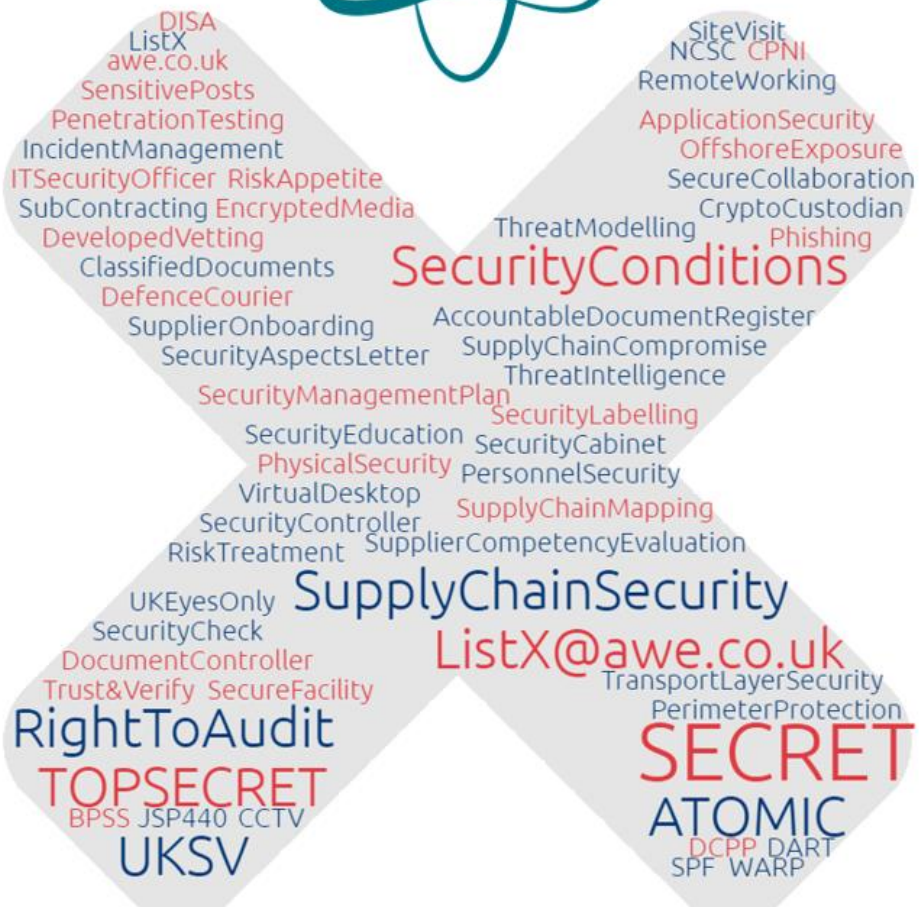

Supply Chain Security

List X Security Guidance

Issue 1 - February 2021

Contents

List X Security Guidance

Introduction

AWE is responsible for the manufacture, maintenance and development of the warheads for Trident, and for supporting nuclear threat reduction.[1]

AWE is a Contracting Authority for the issue of Ministry of Defence contracts. issue MoD contracts. This document outlines the security arrangements for AWE's List X community - those suppliers who are working on AWE contracts which require them to hold or create information or material classified at either Secret or Top Secret.[2]

List X Engagement

Subject to an approved business requirement, AWE will engage directly with a prospective List X supplier to assess the suitability of the physical and technical environment which will be required to deliver the specified service; to implement the appropriate personnel security controls and supporting corporate arrangements; and the handling of classified assets.

Typical stages of the List X lifecycle are shown below:

- **Onboarding**. Identification of a suitable supplier with the requisite skills and capability to deliver a specified service; commercial negotiations; and initial guidance about List X arrangements.

- **Pre-Approval**. Implementation of any requisite physical, personnel or supporting technical security measures identified. AWE will provide guidance and assistance where required, including access to MoD accreditation authorities in respect of the establishment, operation and approval of any classified IT systems; and to the appropriate physical security standards issued by CPNI (Centre for the Protection of National Infrastructure) [3].

- **Approval**. AWE will conduct an inspection of all security aspects before arranging for a facility to be given List X status. MoD authorities will provide approval ("Accreditation") for the operation of any classified IT systems (see "*Classified IT Systems*").

---

[1] See: https://www.awe.co.uk/what-we-do/

[2] There are three HMG security classifications: OFFICIAL, SECRET and TOP SECRET. They indicate the increasing threats to, and sensitivity of information and other assets. Technical, physical, personnel and procedural controls increase at each Tier. List X arrangements also apply when non-UK material which continues to be marked CONFIDENTIAL is at risk.

[3] See: https://www.cpni.gov.uk/physical-security This is the public-facing website; access to additional resources will be facilitated by AWE.

- **Active**. AWE will maintain regular contact with all our active List X community and will conduct periodic surveillance visits to confirm that effective and acceptable security mechanisms remain in place, and that any material provided to the List X supplier is properly accounted for.

- **End of Contract**. At the end of a specific engagement AWE will ensure that all classified material is recovered. It may be appropriate to place List X suppliers into an inactive state if between specific engagements, in order to maintain an ability to return to an active state

Security Aspects Letters

A Security Aspects Letter (SAL) will be issued to the List X supplier, which will set out the nature of the engagement and specific Security Conditions; it will typically include:

- The location(s) where AWE project work may be carried out
- Classification of discrete elements of the project
- Nationality requirements
- Required clearance levels
- Reporting of security incidents

Company Security Instructions

Appropriate guidance and procedures should be put in place to ensure that staff are aware of their roles and responsibilities in handling classified material securely.

Security Appointments

List X suppliers MUST make a number of mandatory appointments. These include:

- **Board Level Contact**. A Company Director (or equivalent) with overall responsibility for security; this person MUST be a UK National.

- **Security Controller**. A UK National who is responsible for all day-to-day aspects of security.

Where relevant, a number of other appointments may be necessary, including:

- **Security Clearance Contact**. Responsible for managing individual security clearances (see "*National Security Vetting*").

- **ATOMIC Liaison Officer**. Responsible for the security of any ATOMIC information which may be issued to the supplier.

- **Crypto Custodian**. Responsible for the management (receipt, storage and distribution) of cryptographic material. If this role is relevant, an **Alternative Crypto Custodian** must also be appointed.

- **IT Security Officer**. Responsible for the security management and oversight of any classified IT systems (see "*Classified IT Systems*" below).

- **Document Controller**. Responsible for accounting for holdings of classified documents.

AWE can provide further guidance, including access to relevant agencies and material. The **Defence Industry Security Association** (DISA) offers training covering a number of these roles; AWE will sponsor DISA membership on request.[4]

Personnel Security

Appropriate pre-employment checks should be carried out for all staff employed within our List X community, which should conform to the Baseline Personnel Security Standard (BPSS).[5]

There should be a supporting personnel security policy in place, to include expected standards of personal responsibilities and accountabilities. Nationality requirements will normally be specified in Security Aspects Letters, eg the need to employ UK or other acceptable Nationals on classified project work.

National Security Vetting

AWE contracts (and Security Aspects Letters) will specify the levels of clearance required for List X supplier staff to work on AWE projects.

United Kingdom Security Vetting (UKSV) provides the UK's National Security Vetting (NSV) services and the issue of individual security clearances.[6]

Protective Security

AWE will facilitate access to local police force Counter Terrorism Security Advisors (CTSAs) who can provide help, advice and guidance on protective security measures.[7]

---

[4] See: http://www.thedisa.org/training.htm

[5] See: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard

[6] See: https://www.gov.uk/government/organisations/united-kingdom-security-vetting/about

[7] See: https://www.gov.uk/government/publications/counter-terrorism-support-for-businesses-and-communities/working-with-counter-terrorism-security-advisers

Physical Security

General security requirements for List X are published by HMG.[8] AWE will provide further guidance as required, which may include:

- Specification of security standards for premises
- Facilitating access to approved security equipment
- Intrusion detection, alarm and response mechanisms

Secure Data Exchange

AWE will determine and agree secure exchange mechanisms in order to transfer classified data (or material) to/from the List X site, which will normally be subject to a security management plan.

Classified IT Systems

The MoD is responsible for approving the design, security management, and operation of any supplier-operated IT systems which process data above the Official Tier, and for system accreditation.[9]

Sub-Contractors

If a List X supplier is considering sub-contracting any aspect of classified at SECRET or above permission must be sought from AWE; any such sub-contractor will themselves be required to go through List X accreditation.

Security Monitoring

List X suppliers, and any associated elements of the AWE Supply Chain, may be subject to open-source security monitoring carried out by AWE or their agents.

Security Incidents

If there has been any compromise or suspected compromise of AWE data or assets, of the failure or degradation of a security control, the List X supplier must inform AWE at the earliest opportunity, and be prepared to facilitate any investigation or incident management procedure which AWE their agents, or a national agency may carry out.

---

[8] See: https://www.gov.uk/government/publications/security-requirements-for-list-x-contractors

[9] See: https://www.gov.uk/guidance/defence-security-and-assurance-services-defence-industry-list-x

Industry Security Notices

The MoD publishes Industry Security Notices (ISNs) to provide guidance and direction across a range of security topics.[10] AWE will augment and provide additional guidance and direction where appropriate.

Security Advice

AWE's **List X Security Manager** will be the focal point for guidance, security assessments and oversight throughout any List X engagement, including the co-ordination of any security management plans

Work in the Official Tier

Security requirements for suppliers working in the Official Tier are published in **Cyber Security for the AWE Supply Chain**, available from the AWE website.[11]

Further Guidance

All external links contained in this document are correct at the time of production but are subject to change.

For further guidance in respect of List X facilities and security arrangements please contact:

ListX@awe.co.uk

For any aspects of working in the Official Tier please contact:

SupplyChainSecurity@awe.co.uk

[10] See: https://www.gov.uk/government/publications/industry-security-notices-isns

[11] See: https://www.awe.co.uk/app/uploads/2020/08/Cyber-Security-for-the-AWE-Supply-Chain-V2-August-2020.pdf