Cyber Security for the AWE Supply Chain

Issue 2 - August 2020

Contents

Cyber Security for the AWE Supply Chain

Part 1: AWE's Supply Chain Risk Management Approach

Introduction

AWE is responsible to the Ministry of Defence (MoD) for protecting some of the UK's most critical information assets.

This document sets out AWE's requirements in order that information classified in the Official Tier is effectively protected and handled appropriately when shared with, or created by, all elements of the AWE Supply Chain.

The AWE Supply Chain

AWE's supply chain risk management approach - and the application of these requirements - extends beyond just those companies who are in direct (prime) contract with us. It applies wherever there is risk to AWE, and includes:

- direct (prime) suppliers to AWE
- sub-contractors[1] to our direct (prime) suppliers
- specialist IT and other companies providing security services, system management and/or administration support to our suppliers or their sub-contractors
- cloud-based and other collaborative environments used by AWE, our suppliers and/or their sub-contractors to work on AWE projects and/or support our capabilities
- critical business applications used to support AWE projects or capabilities

AWE will determine the application of these requirements in respect of individual projects and contractual arrangements, including the establishment of a proportionate risk management approach for lower tier sub-contractors.

The Official Tier

OFFICIAL is one of three Government Security Classifications.[2] The Official Tier is where AWE conducts its own day-to-day business, as well as having a large amount of project and other supporting work carried out by our Supply Chain.

Some Official information will be of a more sensitive nature and be identified as requiring additional supporting technical and procedural controls to reinforce the Need-to-Know principle: it may bear an OFFICIAL-SENSITIVE (OS) security marking; or be so identified by specific handling instructions or Security Conditions.

---

[1] The term "sub-contractor" throughout this document includes both direct and any subsequent (lower-tier) suppliers; the extent of AWE risk and risk management requirements will be determined on a case-by-case basis.

[2] The three classification tiers are OFFICIAL, SECRET and TOP SECRET. They indicate the increasing threats to, and sensitivity of, information; technical, physical and supporting procedural controls increase for data and material classified in the upper tiers.

Cyber Essentials

The National Cyber Security Centre (NCSC) Cyber Essentials scheme is designed to guard against the most common internet-based cyber security threats. It demonstrate a commitment to cyber hygiene, and is recognised as commercial good practice. Suppliers should recognise that a growing number of organisations, especially those in the public and critical national infrastructure sectors, are specifying that their suppliers meet certification against this scheme as a minimum business requirement.

AWE expects all suppliers working at OFFICIAL (except sole traders/micro-sized companies with less than 10 staff) to be certified at the basic level of the scheme (CE).

For larger companies, or for those working with personally identifiable or other sensitive data (including OS), Cyber Essentials Plus (CE+) certification is expected and may be specified.[3]

Classified Projects

Suppliers engaged on projects involving information/material (classified above the Official Tier) under the auspices of List X will be subject to additional controls, approvals and assurance arrangements.[4] Any IT systems used to process data at these levels will be subject to MoD accreditation.

Further guidance is available from AWE.

Defence Cyber Protection Partnership and Cyber Profiles

The Defence Cyber Protection Partnership (DCPP) is a pan-Defence collaboration scheme which sets out a range of control measures, and calls for MoD Contracting Authorities, such as AWE, to assign Cyber Profiles to suppliers.

AWE has aligned these profile definitions against cyber security expectations based on the size of the supplier company; these are shown in the table below, and the associated specified or expected security controls are described more fully in Part 2.

	Sole Trader	**Micro Company** (2-10 staff)	**Small Company** (10-50 staff)	**Medium Company** (50-250 staff)	**Large Company** (250+ staff)
Cyber Profile	BASELINE	BASELINE	VERY LOW	LOW	MODERATE
OFFICIAL: Cyber Essentials Certification	CE Recommended		CE	CE+	CE+
OFFICIAL-SENSITIVE: Cyber Essentials Certification	CE+ may be specified by AWE on case-by-case basis		CE+	CE+	CE+

[3] Where additional independent assurance arrangements are in place (eg penetration testing) this can offset the need for CE+

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

Sole Traders & Micro-Sized Companies

AWE expects sole traders and micro-sized companies (up to 10 staff) to operate sensible cyber hygiene (Baseline Measures), as described by NCSC in their Sole Trader guidance [5] and explained more fully in Part 2 of this document. Whilst not mandated by AWE for working at OFFICIAL, CE certification is recommended for both Sole Traders and Micro companies; and CE+ may be appropriate in some cases when working at OS or with other sensitive material. This may be determined by AWE and agreed with the supplier on a case-by-case basis.

Small Companies

In addition to the Baseline Measures, small SMEs (10-50 staff) are required to operate at the VERY LOW Cyber profile, and to have CE certification. Depending on the nature of the work undertaken, some small SMEs may be required to operate at the higher LOW Cyber Profile with CE+ certification.

Medium Sized Companies

At this level (50-250 staff) CE+ is expected, as are proportionately increased governance, security management, and supporting secure working and information handling arrangements, to meet the LOW Cyber Profile.

Large and Very Large Companies

We expect larger enterprises to conform to the MODERATE Cyber Profile, which involves the implementation of a commensurate increase in governance, proactive security management, security monitoring etc; more robust evidence of independent assurance; and of setting and assuring security requirements for any sub-contractors. NCSC provides additional guidance.[6]

Sub-Contractors

We understand that many of our suppliers will need to outsource or sub-contract elements of their work for us. Our standard contractual terms require outsourcing and sub-contracting to be visible to us, and in some cases, this will be subject to AWE approval.

Prospective Suppliers

When seeking tenders for prospective work AWE will provide supporting guidance about how any documentation we provide for information and/or tendering purposes should be handled.

We recognise that AWE documentation may need to be shared more widely with prospective sub-contractors or subsidiary equipment and/or service suppliers and expect that appropriate handling instructions will be flowed down.

We expect AWE-identifiable material to be handled with a degree of discretion and commercial sensitivity.

[5] See: https://www.ncsc.gov.uk/section/information-for/self-employed-sole-traders

[6] See: https://www.ncsc.gov.uk/section/information-for/large-organisations

IT Support Companies

We understand and accept that many of our smaller suppliers rely on a third party for the provision, operation, management and/or administration of their IT estate. Commensurate with their size, we expect any IT support company to be operating to at least the same Cyber Profile as our supplier or sub-contractor; in some cases it will be more appropriate that they should implement enhanced levels of security governance and management.

In most cases this will mean that, notwithstanding their size, IT support companies will be expected to be certified at CE+ and/or be able to demonstrate acceptable independent assurance of their IT security arrangements.

Global Corporate Organisations/Non-UK Suppliers

We recognise the benefits that come from being able to source goods and services from non-UK companies, and those that operate in a global market. We understand that in many cases governance, employment and technical control arrangements may be at variance with those identified in this document, and AWE is amenable to considering equivalent certifications etc.

Right to Audit and Security Assessments

AWE will conduct security assessments of its supply chain at a number of levels. During the onboarding (or at a periodic contract renewal or change of contract point) suppliers will be asked to submit a conformance statement and/or evidence of security credentials.

AWE reserves the right to undertake site security visits, which may extend to sub-contractors and IT support providers. These will typically be carried out when:

- Personal or sensitive data is at risk
- Where there a higher degree of risk to our operations and/or our capability
- When data is at risk offshore
- When novel solutions are proposed

The aim of our security assessments is for AWE to consider whether cyber and other security arrangements are acceptable and within risk appetite, and/or to agree proportionate risk treatment actions. When sensitive evidence is disclosed, this can be provided under Non-Disclosure terms.

In some cases, AWE may specify that additional independent testing is carried out, which will be conducted in agreement with the supplier and their agents. Further visits may be carried out at periodic intervals, based on the level of risk and AWE's confidence in the supplier's ability to maintain an acceptable security posture.

Suppliers working under List X arrangements will normally have surveillance visits carried out at least annually.

Cloud Services

Where cloud services are in use, suppliers should be satisfied that the cloud environment has been established in accordance with a recognised set of security standards, eg the NCSC Cloud Security Principles.[7]

[7] See: https://www.ncsc.gov.uk/collection/cloud-security

Software-as-a-Service & Critical Business Applications

Where AWE business is being conducted or supported via a Software-as-a-Service (SaaS) solution, that service MUST be subject to a reasonable degree of due diligence, including the provision of satisfactory independent testing – see NCSC guidance on SaaS security.[8]

Use of SaaS solutions will normally be subject to AWE approval.

Prime Assurance & Supplier Due Diligence

AWE expects that where a supplier sub-contracts work (including outsourcing the management of IT systems) it will have carried out satisfactory due diligence on third parties.

Suppliers are required to demonstrate Supply Chain Mapping of sub-contractors (and other lower tier third parties) – as well as relevant cloud hosting, collaborative environments, offshore components, critical applications and SaaS solutions – in order to present AWE with visibility of where AWE data is at risk. Further guidance is available from AWE.

Offshoring

Where there is a requirement – with a business benefit – to our work being offshored, this MUST be approved by AWE.

Suppliers will understand that due to the nature of our work, there will be some jurisdictions where offshoring will not be possible, though in the Official Tier we operate within a realistic risk appetite and will be amenable to considering appropriate offshoring.

Further guidance is available from AWE.

Secure Connectivity with AWE

AWE will seek to establish secure connectivity arrangements with all suppliers. Where personal or sensitive, including OFFICIAL-SENSITIVE, data is being exchanged, data MUST be protected in transit (eg by encrypted email or media) to a level acceptable to AWE. More detailed guidance is available from AWE.

Personal Devices

It is not permitted to use personally owned devices to conduct AWE-related business, except in the following circumstances:

- **Bring-your-own-Device (BYOD)**. Limited use of personal devices is acceptable within the confines of an acceptable BYOD policy. NCSC provides guidance on establishing and operating a BYOD regime.[9]

- **Desktop Virtualisation**. Use of an assured solution which allows the presentation of a corporate desktop to a non-corporate device.

Further guidance is available from AWE

[8] See: https://www.ncsc.gov.uk/collection/saas-security

[9] See: https://www.ncsc.gov.uk/collection/mobile-device-guidance/bring-your-own-device

Physical Security

Work in the Official Tier may be conducted in commercial or domestic premises. Physical security controls (barriers/procedural measures/working arrangements) should be such that unauthorised access to AWE data or material is prevented, and that our work is carried out with discretion.

OS documents/material should be kept under lock and key when not in use and disposed of securely when no longer required. See the Official Tier Control Framework at Part 3.

Personnel Security

Pre-employment checks should be carried out with staff cleared to the Baseline Personnel Security Standard (BPSS) [10] or equivalent. Personal responsibility for the implementation of security procedures and adherence to policy should be reinforced through training and company policies.

Nationality requirements may be specified for work at OS; further guidance is available from AWE.

Classification Labelling

There is no requirement to mark OFFICIAL documents with a security label. OS documents (including emails) should be marked "OFFICIAL-SENSITIVE".

Supplier Systems on AWE sites

Our suppliers may operate their own IT systems on our sites subject to the following guidelines:

- **Laptop computers and mobile devices**. These may be brought onto site and operated in accordance with site security requirements. This will involve equipment being registered with AWE and being used in accordance with relevant zoning policies, signage and any operating limitations imposed by AWE. Guest wireless/wired services are available to facilitate external connectivity.

- **Local area networks**. These may be established in appropriate locations, subject to AWE approval and acceptable security management arrangements.

More detailed guidance is available from AWE.

Security Incidents

If there has been any compromise or suspected compromise of AWE data, or the failure or degradation of a security control which is designed to assure the confidentiality, integrity or availability of AWE data or other assets, the supplier MUST inform the relevant AWE sponsor at the earliest opportunity.

Suppliers should be prepared to facilitate any investigation which AWE, their agents, or a national agency, may carry out.

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

Security Monitoring

Suppliers (and other elements of the AWE Supply Chain) may be subject to open-source security monitoring carried out by AWE or their agents.

Reference to AWE Projects

Publicising work carried out for AWE – eg as reference sites, in case studies, in general publicity, including via use of social media channels – is not permitted without prior approval from AWE.

References and Resources

A number of recommended and referenced resources are contained in Part 4. Where URLs have been provided these are correct at time of writing but are subject to change.

AWE Further Guidance

Any requests for variance in any of the control measures specified in this document, or additional guidance, should be made to AWE at: **SupplyChainSecurity@awe.co.uk**

Part 2: Cyber Profiles and Security Controls

The following security controls are AWE's expected minimum standard. It is within our risk approach to consider appropriate alternatives or mitigations on a case-by-case basis.

SECURITY BASELINE

It is assessed that the large majority of successful attacks against UK businesses and citizens would have been mitigated by the implementation of good practice (Baseline Measures). Our suppliers who are sole trader or micro businesses are required to have implemented these basic cyber hygiene controls.

- **Boundary Protection**. An internet gateway (router) or a firewall device will provide technical protection between your system and the outside world. Default settings should be changed. If a separate hardware firewall is used it needs to be correctly configured.

- **Secure Configuration**. Computers are not secure out of the box. Unwanted software, services and accounts should be removed or disabled, and default settings changed. Only reputable software should be used. Laptop computers MUST be encrypted.

- **Patch Management**. Operating system and application software should be kept up to date in accordance with manufacturer releases. Applications no longer required should be removed. Devices which are no longer supported should not be used.

- **Access Control**. Computer use should be on a least privilege basis. Users should only have the access they need. Administrative access should only be used for administration functions. Strong (and unique) passwords should be used. Multi-factor authentication should be enabled for any administrative access.

- **Malware Protection**. Anti-Virus software should be installed, kept up to date, and run regularly. Business-critical data should be kept backed up. USB and other removeable media should be managed.

- **Security Awareness**. Be wary of malicious emails (eg phishing attacks), and the use of public wireless access. Conduct any work for AWE with discretion and a degree of privacy.

VERY LOW CYBER PROFILE

In addition to the Baseline Measures, at this level **Cyber Essentials** certification is required. NCSC provides additional guidance for small businesses[11].

LOW CYBER PROFILE

In addition to the Baseline Measures, companies at this level are required to have Cyber Essentials Plus, and expected to have an increasing level of security in place, eg:

- **Governance**. Security roles assigned; security policies and procedures implemented.

[11] See: https://www.ncsc.gov.uk/collection/small-business-guide

- **Security Culture and Awareness**. Staff responsibilities explained; training provided for all staff.

- **Protecting Information Assets**. AWE data subject to authorised access control arrangements. Removable media controls; endpoint protection; IT systems subject to active management.

- **Physical and Personnel security**. Effective controls in place to protect commercial premises; reporting of security violations to be enabled; and implementation of security policies to be required under contractual arrangements.

- **Security Incidents**. Security violations, or failure or compromise of security controls, to be identified and resolved.

MODERATE CYBER PROFILE

In addition to Baseline Measures and the VERY LOW/LOW Cyber Profile controls, larger companies are expected to have enhanced security governance, security management and system security arrangements in place. These should include:

- **Risk Management**. Implementation of a risk management regime; access to appropriately qualified and experienced cyber professional resources, and to relevant threat intelligence.

- **Vulnerability Management**. Active analysis of system configuration and patch levels; remediation of identified vulnerabilities.

- **Penetration Testing**. For UK companies an active and comprehensive testing programme carried out under the auspices of the CREST scheme; an equivalent programme for non-UK companies.

- **System Monitoring**. Effective monitoring of information asset access and user behaviours; network and security devices; and of any security enforcing functions.

- **Data Loss Prevention**. Effective controls in place to monitor and detect potential data loss or compromise events.

HIGH CYBER PROFILE

Some companies operating in sectors or on projects which attract a higher level of risk may be required to implement additional security controls, though these will not normally be expected when working in the Official Tier. If required, these will be specified and agreed on a case-by-case basis in discussion with AWE.

SECURITY CONDITIONS

In some circumstances additional controls or other risk treatment may be specified by AWE; these will normally be set out as “Security Conditions” contained within a Security Aspects Letter, and will be a contractual requirement. These will need to be flowed down to any sub-contractor, and/or where appropriate cascaded throughout the relevant supply chain.

Part 3: AWE Official Tier Control Framework

Information and other AWE assets in the Official Tier face threats broadly similar to any large UK private company, where information and material should be protected from adversaries with bounded resources and capabilities. Attackers may include hacktivists, pressure groups, investigative journalists, and criminal groups.

AWE takes a risk-based approach in this Control Framework to recommend and/or specify proportionate protection measures. Controls, whether technical or procedural, are not designed to provide absolute assurance against more capable and determined threat actors, but to provide robust and effective measures to make it difficult, time-consuming and expensive to gain unauthorised and undetected access, and/or to otherwise compromise our assets.

<table>
<tr><th></th><th>OFFICIAL</th><th>OFFICIAL-SENSITIVE[12]</th></tr>
<tr><td>General</td><td>Proportionate risk may be taken to achieve business objectives

Impact of compromise would not cause significant harm</td><td>In addition:

Where need-to-know should be enforced and a higher degree of assurance is required</td></tr>
<tr><td>Security Outcome</td><td>Legal and regulatory requirements to be met

Promote responsible sharing and discretion

Proportionate and appropriate controls to be in place

Make accidental or opportunistic compromise unlikely</td><td>In addition:

Deter deliberate attempts at compromise; make it likely that those responsible will be identifiable

Detect and resist deliberate attempts to compromise specified and/or aggregated data, making it highly likely that any compromise will be identified, and appropriate responses initiated</td></tr>
<tr><td>Physical Security</td><td>Proportionate good practice against accidental or opportunistic compromise</td><td>Deter deliberate compromise by forced and/or surreptitious attack</td></tr>
<tr><td rowspan="2">Personnel Security</td><td colspan="2">Appropriate recruitment checks – BPSS or acceptable equivalent

Personal responsibility reinforced through training and company policies</td></tr>
<tr><td>Access by authorised persons for legitimate business reasons</td><td>Assurance that access is only by known and trusted individuals with a need to know

Nationality sensitivity may apply</td></tr>
<tr><td>Document Handling</td><td>Proportionate measures to control authorised access</td><td>Consider whether documents need to be made accountable</td></tr>
</table>

[12] To include work on other “sensitive” material as specified by AWE.

	OFFICIAL	OFFICIAL-SENSITIVE[12]
Security Labelling	Not required	Documents and Emails MUST be labelled OFFICIAL-SENSITIVE
Document Disposal	Normal recycling	Shredded or torn in such a way as to make reconstitution efforts disproportionate
IT systems	Protect against deliberate compromise by automated or opportunistic attack Detect and respond to actual or attempted compromise	*In addition*: Deter deliberate compromise by capable threat actors Assurance that information is protected by specified controls Positive action response to incidents
Email	Commercial email to any legitimate recipient	MUST be protected in transit by acceptable encryption
Media transfer	Permitted	MUST be protected in transit by acceptable encryption
Document Transmission	Royal Mail or reputable courier permitted No OFFICIAL/OFFICIAL-SENSITIVE marking to be shown on envelope	
Security Incidents	Any compromise or suspected compromise to be managed internally; AWE to be informed.	AWE to be made aware at earliest opportunity; AWE may specify additional investigation and/or incident management measures
Secure Voice[13] Telephone	Can be discussed freely on all types of phone	Discussion not to take place with, or within earshot of, unauthorised persons
Video conferencing	Permitted	Permitted within and between OS-approved organisations, subject to AWE approval
Cloud Services[14]	Permitted; AWE to be informed	Permitted, subject to AWE approval
Sub-Contracting	Permitted; AWE to be informed	Permitted, subject to AWE approval
Offshoring	Permitted, subject to AWE approval	
Remote working	Permitted subject to implementing discretion and privacy arrangements	

[13] See: https://www.ncsc.gov.uk/guidance/secure-voice-official

[14] To include Cloud Hosting; SaaS solutions; use of Collaborative Working Environments; etc

Part 4: Cyber Resources and References

The following sources of additional advice are recommended. URLs are subject to change.

HM Government
Department for Business, Energy & Industrial Strategy
Ministry of Defence

HMG guidance on cyber security; the Government Security Classifications; on BPSS; the Defence Cyber Protection Partnership; on List X security requirements; and issue of Industry Security Notices. See:

https://www.gov.uk/government/cyber-security
https://www.gov.uk/government/publications/government-security-classifications
https://www.gov.uk/guidance/defence-cyber-protection-partnership
https://www.gov.uk/government/publications/security-requirements-for-list-x-contractors
https://www.gov.uk/government/publications/industry-security-notices-isns

National Cyber Security Centre
a part of GCHQ

The UK's National Authority for Information Assurance. An extensive range of technical security guidance covering advice for Sole Traders, SMEs and Large Companies; Cloud Security principles; Endpoint Protection; etc. See:
https://www.ncsc.gov.uk/section/advice-guidance/all-topics

CYBER ESSENTIALS
CYBER ESSENTIALS PLUS

The Cyber Essentials scheme is explained at:
https://www.ncsc.gov.uk/cyberessentials/overview

IASME CONSORTIUM

IASME Consortium (NCSC's scheme partner) explains how to get certified to Cyber Essentials or Cyber Essentials Plus. There is also guidance about IASME's Governance Model. See:

https://iasme.co.uk/cyber-essentials/
https://iasme.co.uk/iasme-governance/

CPNI
Centre for the Protection of National Infrastructure

CPNI provides guidance on physical and personnel security, and on security awareness. It also publishes the Catalogue of Security Equipment. See:

https://www.cpni.gov.uk/physical-security
https://www.cpni.gov.uk/personnel-and-people-security
https://www.cpni.gov.uk/cse-categories

CiSP

The Cyber Security Information Sharing Partnership is an industry and government initiative to exchange real time cyber threat information & provide situational awareness. **AWE will sponsor access to CiSP for our suppliers and their IT support providers on request**. See:
https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

NIST
National Institute of Standards and Technology

NIST publishes US Government standards on information technology and cyber security. See: https://www.nist.gov/topics/cybersecurity

Get Safe Online is a resource, jointly funded by government and the private sector, to promote internet security, and which contains guidance for businesses at: https://www.getsafeonline.org/business/

The ISO27001 standard is recognised as the benchmark for Information Security Management Systems; ISO28000 specifies a management system for supply chain assurance. See:

https://www.iso.org/isoiec-27001-information-security.html
https://www.iso.org/standard/44641.html

CREST is recognised as the benchmark for security testing, with approved providers independently accredited to deliver penetration testing; web application; and other security services.
See: https://service-selection-platform.crest-approved.org/

DISA is an industry association for suppliers working in the defence sector. **AWE will sponsor applications for DISA membership on request**. See: http://www.thedisa.org/

The ISF has guidance on governance, supply chain risk management; publishes a standard of good practice for information security; and a risk assessment methodology. See: https://www.securityforum.org/about/

CIS provides guidance on cyber security, including the "20 CIS Controls".
See: https://www.cisecurity.org/controls/cis-controls-list/

CSA provides guidance for secure cloud computing.
See: https://cloudsecurityalliance.org/

The Open Web Application Security Project's "Top Ten" can be used for secure application development. See: https://owasp.org/www-project-top-ten/

The Mitre ATT&CK framework describes typical tactics, techniques and procedures used by capable adversaries. See: https://attack.mitre.org/

The SANS Institute is a recognised leader in cyber technical training and certification. See: https://www.sans.org/

The Cyber Body of Knowledge underpins professional training and education for the cyber security sector. See: https://www.cybok.org/