AWE NUCLEAR SECURITY TECHNOLOGIES

Supply Chain Security

Security Requirements for the AWE Supply Chain
Technical Supplement

Issue 1: September 2025

Contents

1. Purpose

1.1. The purpose of this Technical Supplement is to provide external partners the guidance on working securely with AWE, and the expected security controls.

The target audience for this document is those responsible for information security management at your organisation.

1.2. This Technical Supplement must be read in conjunction with **Security Requirements for the AWE Supply Chain**[1].

1 See Supply Chain Security:
https://www.awe.co.uk/our-supply-chain/our-suppliers/supplier-assurance/

2. Security Control Framework and Security Profiles

2.1. Information and other AWE assets in the Official Tier[2] face threats broadly similar to any large UK private company, where information and material must be protected from threat actors.

2.2. Threat actors may include but are not limited to: state actors; pressure groups; opportunistic actors; hacktivists; organised crime; investigative groups; and staff who pose an insider risk.

2.3. AWE takes a risk-based approach in this Security 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 compromise our assets.

2.4. Our Suppliers - and associated third parties and subcontractors – will be expected to meet and maintain a range of proportionate security measures. These measures, covering cyber, physical, personnel and procedural security arrangements, will be specified as a Security Profile, as identified in Table 1: Security Profiles.

2.4.1. Detailed Technical Controls are identified in Table 2: Technical Control Requirements, generally based around the key security controls in Section 3 – Security Controls.

2.4.2. Foreign Ownership Control and Influence (FOCI) and nationality restrictions apply and must be declared to AWE prior to any work or contract for AWE review and approval. Any change while under contract must also be declared to AWE.

2.4.3. All those persons directly engaged on AWE work – with access to Official Assets – should meet a minimum recruitment control of the Baseline Personnel Security Standard (BPSS)[3] or an equivalent[4] acceptable to AWE.

2.4.4. Offshore exposure (outside the UK) of any AWE work must be declared prior to any work or contract for AWE review and approval.

2.4.5. There is a maximum classification of work that can be undertaken against an assigned Security Profile.

2.4.6. The use of Cloud hosted services is permissible following a review and approval by AWE.

2.4.7. Technical security controls should be implemented to best practice e.g. achieving Cyber Essentials (CE) or Cyber Essentials Plus (CE+) or Equivalent[5].

2.4.8. While not mandatory, we encourage our UK suppliers to pursue certification through the MoD's Defence Cyber Certification (DCC)[6] scheme; we also encourage our US suppliers to consider obtaining the Department of Defense's Cyber Security Model Certification (CMMC)[7]. Certification should be sought at an appropriate level to reflect the supplier's assigned security profile.

2.5. The Supplier shall, for each security requirement referenced in Table 2, ensure they have a documented and implemented control in place with auditable evidence.

2 The Official Tier is where AWE conducts day-to-day business.
3 See: https://www.gov.uk/government/publications/united-kingdom-security-vetting-clearance-levels/national-security-vetting-clearance-levels
4 BPSS equivalence includes recruitment controls covering: Identity Verification; Nationality and Immigration (right to work) status: Employment History (3 years minimum): and a Criminal Record Check (unspent convictions).
5 http://www.ncsc.gov.uk/cyberessentials/overview
6 See: https://www.gov.uk/guidance/cyber-security-model and https://iasme.co.uk/defence-cyber-certification/
7 See: https://dodcio.defense.gov/cmmc/About/

Table 1: Security Profiles

Security Profile (SP)	Technical Controls	FOCI and nationality requirements	Personnel Security Controls	Offshore Exposure	Maximum Classification	Use of Cloud
SP0	Level 0 (baseline) (CE or equivalent[8] expected)	Restrictions apply, seek approval	BPSS (or equivalent[3]) Expected	Restrictions apply, seek approval	OFFICIAL including for public release	Permissible following review in line with Technical Controls
SP1	Level 1 (CE or equivalent[8] required. CE+ advised)	Restrictions apply, seek approval	BPSS (or equivalent[3]) Expected	Restrictions apply, seek approval	OFFICIAL	Permissible following review in line with Technical Controls
SP2	Level 2 (CE+ or equivalent[9] required)	Restrictions apply, seek approval	BPSS (or equivalent[3]) Minimum	Restrictions apply, seek approval	OFFICIAL-SENSITIVE	Permissible following review in line with Technical Controls
SP3	Level 3 (CE+ or equivalent[9] and increased controls)	Restrictions apply, seek approval	BPSS (or equivalent[3]) Minimum	Restrictions apply, seek approval	OFFICIAL-SENSITIVE inc Personally Identifiable Information (PII)	Permissible following review in line with Technical Controls

8 Cyber Essentials (CE) equivalence can be achieved by providing suitable explanation, evidence and demonstration of the 5 key areas of the Security Baseline Measures (3.1). Suitable equivalence could also be similar certification from a recognised body outside the UK, requiring AWE approval.

9 Additional independent assurance arrangements (e.g. regular penetration testing regime, independent assurances (SOC2) etc.) or recognised equivalent certifications can offset the need for Cyber Essentials Plus (CE+), or evidenced conformance to a recognised control regime (i.e. NIST, EU NIS2, DCC). Suitable explanation, evidence and demonstration of the Level 2 and Level 3 technical controls to meet SP2 and SP3 requirements may also be suitable.

3. Security Controls

3.1. Security Baseline Measures

Cyber attacks can significantly disrupt an organisation's operations, put sensitive business information at risk, cost money and damage reputation. The large majority of successful attacks would have been mitigated by the implementation of basic cyber hygiene controls and good practice. The expected Security Baseline for all AWE suppliers is to implement the following control measures:

3.1.1. Firewalls and routers

Implement and manage to make sure that only secure and necessary network services can be accessed from the Internet. AWE suppliers must protect every device with a correctly configured firewall (or network device with firewall functionality).

3.1.2. Secure Configuration

Ensure that computers and network devices are properly configured to reduce vulnerabilities and provide only the services required to fulfil the necessary function. AWE suppliers must proactively manage computers and network devices.

3.1.3. Security Update Management

Ensure that devices and software are not vulnerable to known security issues by keeping software up to date with latest versions and patches.

3.1.4. User Access Control

Ensure that user accounts are assigned to authorised individuals only, and provide access to only those applications, devices, and networks a user needs to carry out the role. AWE suppliers must be in control of user accounts and the access privileges that allow access to company data and services, including those relating to AWE projects by applying the 'need to know' principle. This also includes third party accounts – for example accounts used by any support services. Suppliers need to understand how user accounts authenticate and manage the authentication accordingly. As well as providing an extra layer of security for passwords that aren't protected by the other technical controls, the use of 2-step verification (2SV) should be implemented to give administrative and privileged accounts extra security, as well as accounts that are accessible from the Internet.

3.1.5. Malware Protection

To restrict execution of known malware and untrusted software from causing damage or accessing data, AWE suppliers must make sure that a suitable malware protection mechanism is active on all devices. In most modern products these options are built into the software supplied. Alternatively, specific products can be purchased from a third-party provider. In all cases the software must be active and kept up to date in accordance with the vendors instructions. Regular backups of supplier systems must also be conducted.

3.2. SP0

Along with the Security Baseline Measures, Cyber Essentials certification or equivalent[3] is expected.

3.3. SP1

In addition to the Security Baseline Measures and Security Profile 0, companies at this level are required to have Cyber Essentials certification or equivalent[3] as a minimum with CE+ advised.

3. Security Controls continued

3.4. SP2

In addition to the Security Baseline Measures and Security Profiles 0 and 1, companies at this level are required to have Cyber Essentials Plus certification or equivalent[4], and to have an increased level of security in place due to the need to protect sensitive information. This includes evidence and demonstration of;

3.4.1. Governance

Security roles assigned; security policies and procedures implemented.

3.4.2. Security Culture and Awareness

Staff responsibilities explained; training provided for all staff.

3.4.3. Protecting Information Assets

AWE data subject to authorised access control arrangements (see 3.1.4). Removable media controls; endpoint protection; IT systems subject to active management.

3.4.4. 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 for those personnel managing more sensitive AWE assets.

3.4.5. Security Incidents

Suitable security incident management policies and procedures are to be in place to ensure security violations, or failure or compromise of security controls, can be identified and resolved. Any compromise or suspected compromise of AWE assets must be reported to AWE as soon as possible.

3.5. SP3

In addition to Security Baseline Measures and the SP0, SP1 and SP2 controls, organisations required to meet the SP3 controls are to have enhanced security governance, security management and system security arrangements in place to protect more sensitive AWE information and assets. This includes evidence and demonstration of;

3.5.1. Risk Management

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

3.5.2.Vulnerability Management

Active analysis of system configuration and patch levels; remediation of identified vulnerabilities.

3.5.3.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.

3.5.4. System Monitoring

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

3.5.5. Data Loss Prevention

Effective controls in place to monitor and detect potential data loss or compromise events.

3. Security Controls continued

3.6. Some companies engaged 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 (SP0-SP3). If required, these will be specified and agreed on a case-by-case basis in agreement with AWE.

3.7. 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 (SAL) 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.

3.8. The table below is AWE’s implementation of the Control Requirements set out in Defence Standard (Def Stan) 05-138 Issue 4.[10]

10 See: https://www.gov.uk/government/publications/cyber-security-for-defence-suppliers-def-stan-05-138-issue-4

Table 2: Technical Control Requirements

Control	Level 0: Security Baseline requirements, refer to 3.1. Cyber Essentials or equivalent[3], is expected	
	Level 1	Level 2 and Level 3
Working at OFFICIAL: Cyber Essentials, or equivalent[3], is required. Working at OFFICIAL-SENSITIVE (OS): Cyber Essentials Plus, or equivalent[4], is required.		
Objective A: Managing Security Risk The Supplier has appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to its network, and information systems, including those that protect all company, customer and supplier Data.		
Organisational	Appropriate management policies and processes for security. Security roles and responsibilities are established with effective means to communicate and escalate risks. Appropriate steps taken to identify, assess, understand and remediate security risks. The risk to organisational assets, and the associated processing, storage, or transmission of Data is periodically assessed. Network diagrams are maintained.	*In addition:* Effective security management led at board level. Senior-level accountability for security and delegated authority decision-making. Risk Management process. Level 3 only – Threat intelligence capabilities are part of a risk assessment.
Security Outcome	Documented 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.	*In addition:* Where need-to-know should be enforced and a higher degree of assurance is required. 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
Asset Management and Assurance	Everything required to deliver, maintain or support networks and information systems that support delivery of all data protection functions are determined and understood.	*In addition:* Measures to validate effectiveness of the security in support of functions and which store and/or process data. Regular monitoring of security controls. Automated discovery and management tools maintain an up-to-date, complete, accurate, and readily available inventory of assets to support business Functions and protect Data.

Control	Level 0: Security Baseline requirements, refer to 3.1. Cyber Essentials or equivalent[3], is expected	
	Level 1	Level 2 and Level 3
Physical Security	Physical access to facilities where Data is stored or processed is monitored for unauthorised access and industry standard physical access controls are implemented. Inventory of physical access devices used on premises. Physical access to sensitive areas is restricted to only those with authorised access. Inventory of staff with privileged physical access. Visitor controls applied. Access by authorised persons for legitimate business reasons.	*In addition:* Assurance that physical locations and premises access is only for those with authorised access.
Third-Party Assurance	Security risks from external suppliers are managed and measures in place. Trusted relationships with external service providers are maintained. Trusted suppliers are identified and preferred within the procurement process.	*In addition:* Assurance that access is only by known and trusted individuals with a 'need to know'.
Document Handling	Proportionate measures to control authorised access.	*In addition:* Consider whether documents need to be made accountable with an identified owner and update regime. Register classified documents within a classified information register/asset register.
Security Labelling	It is good practice to label artefacts at OFFICIAL, but not mandatory.	*In addition:* Documents and Emails MUST be labelled OFFICIAL-SENSITIVE at that classification.
Document Disposal	Normal recycling	*In addition:* Shredded or torn in such a way as to make reconstitution efforts disproportionate.

Control	Level 0: Security Baseline requirements, refer to 3.1. Cyber Essentials or equivalent[3], is expected	
	Level 1	Level 2 and Level 3
Objective B: Protecting against cyber attack The Supplier has proportionate security measures in place to protect the networks and information systems supporting all Functions from cyber attack.		
Access and User Management	Access arrangements to assets is documented and understood. Principle of least privilege is implemented. Separation of duties is implemented. Identities and credentials to authorised transactions are managed. Inventory, service and system accounts are each owned and attributable to a single named individual. System users and devices are identified. Remote users acquire appropriate authorisation. Physical and logical access restrictions associated with changes to systems.	*In addition:* MFA is implemented for all users where available, including user/service accounts and privileged accounts (admin). Known devices are trusted and understood. Privileged user access and actions, and identity and access control for users/admins are closely managed. Users accept appropriate warning notices prior to information system access, including information with specific handling requirements. Level 3 only – Automated mechanisms to support the management of system accounts are implemented.
Password Management and Authentication	Secure practices for the secure storage, transmission, and management of first-time and one-time passwords are in use. Deploy technical controls to manage the quality of credentials. Policies and processes are in place to appropriately manage unsuccessful login attempts. Systems to obscure authentication information are configured. Systems to minimise feedback information from failed logons are configured.	*In addition:* Automated mechanisms for the protection and management of passwords for staff and systems. Prevent non-privileged users from executing privileged functions. Administrator credentials are stored through an approved and secured storage mechanism.

Control	Level 0: Security Baseline requirements, refer to 3.1. Cyber Essentials or equivalent[3], is expected	
	Level 1	Level 2 and Level 3
Data	Protect data stored or transmitted electronically. The processing of personal data is conducted in compliance with the GDPR and the flow of all Personally Identifiable Information (PII) and AWE information is monitored and controlled. Cryptography is employed to protect data, and cryptographic keys employed in organisational systems. Publicly accessible data is managed. Inventory of system components using automated tooling for assets that support business Functions and protect Data are documented in an asset register.	*In addition:* Data MUST be protected in transit by acceptable encryption. Assurance that information is protected by specified controls. Good understanding and classification of the data important to the operation of Functions and protection of Data. Protect the confidentiality of soft and hard copies of data, as well as data on mobile devices, through suitable control e.g. encryption, physical security etc. Maintain tooling to monitor and restrict the access and use of: • Removable storage media and devices • External websites • Email Prevent unauthorised and unintended information transfer via shared system resources.
IT Systems and Networks	Controls to protect against replay attacks. Network sessions terminated after inactive communications. Wireless network access controls. Secure network connection controls (e.g. VPN), cryptographic mechanisms, managed access controls points for remote access sessions. Resilience for network and systems and are protected from cyber-attack. Change control procedures are reviewed to manage any system or network changes. Software programs authorised to execute on the corporate environment are identified. Managed list of authorised software. Appropriate internet controls to enforce security on endpoints. Secure network management and communication protocols. Network Time Protocol (NTP) implemented to a recognised authoritative source and clock synchronisation. Control, limit and block connections to and from external systems. Firewalls block every network connectivity path and network service not explicitly authorised by the appropriate Governance policy and procedure. Network segmentation for publicly accessible system components. Media containing diagnostic and/or test programs is checked for malicious code prior to use. MFA to establish non-local maintenance sessions via external network connections and terminate such connections when non-local maintenance is complete.	*In addition*: Unnecessary firewall rules removed or disabled when no longer required.

Control	Level 0: Security Baseline requirements, refer to 3.1. Cyber Essentials or equivalent[3], is expected	
	Level 1	Level 2 and Level 3
Email	Commercial/business email must be used, exchanging only with legitimate recipients. Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) to verify the authenticity of an email's source should be implemented. Appropriate tooling or methods to detect, block and report malicious or spam emails.	*In addition*: Email MUST be protected in transit by acceptable encryption.
Media Transfer/ Removable Media	Permitted where; • Removable storage media and devices are managed and encrypted. • Only corporately owned and/or authorised removable storage media and devices have read/write permissions. The use of removable storage media and devices that are not corporately owned or authorised is prohibited.	*In addition:* MUST be protected in transit by acceptable encryption and packaging. Sanitise before reuse and/ or disposal of the devices, equipment, and removable storage media and devices holding sensitive data, in accordance with industry best practice.
Devices	Full disk level encryption maintained on all endpoints to industry standard solution (e.g., AES-256). Managed mobile devices accessing corporate environment/data (e.g. MDM). Procedures for the secure destruction of data. Acceptable and unacceptable mobile code is managed with controls in place e.g. Secure Development Life Cycle (SDLC) management.	
Document Transmission	Royal Mail or reputable courier permitted. No OFFICIAL/OFFICIAL-SENSITIVE marking to be shown on packaging.	

Control	Level 0: Security Baseline requirements, refer to 3.1. Cyber Essentials or equivalent[3], is expected	
	Level 1	Level 2 and Level 3
Secure Voice[11] Telephone	Can be discussed freely on all types of phones. Usage restrictions and guidance for Voiceover Internet Protocol (VoIP).	*In addition:* Discussion not to take place with, or within earshot of, unauthorised persons.
Video conferencing	Permitted	*In addition:* Permitted within and between OS-approved organisations, subject to AWE approval.
Cloud Services[12]	Permitted at OFFICIAL; AWE to be informed	*In addition:* Permitted, subject to AWE approval
Sub-Contracting	Permitted; AWE to be consulted	*In addition:* Permitted, subject to AWE approval
Offshoring	Permitted, subject to AWE approval	
Remote Working	Permitted subject to implementing discretion and privacy arrangements. Record an updated list of authorised working locations. Technical security controls employed and users are educated to reduce security risks to employees while working outside the organisation's premise.	
Cyber Security Awareness	Regularly review security policies and procedures. Staff have appropriate awareness, knowledge, skills and training and are aware of security risks. Acceptable Use Policy.	*In addition:* Maintain a positive cyber security culture. Staff who support the operation of Functions and protection of Data are appropriately trained in cyber security. Practical exercises in awareness training are aligned with current threat scenarios.
Personnel	Good practice is implemented to allow maintenance personnel to carry out their duties, supervised by qualified personnel. Appropriate background verification, BPSS, and NSV checks are applied where required. Joiners, movers and leavers policy and training and processes to report suspicious activities and/or behaviour.	

11 See: https://www.ncsc.gov.uk/guidance/secure-communication-principles
12 To include Cloud Hosting; SaaS solutions; use of Collaborative Working Environments; etc.

Control	Level 0: Security Baseline requirements, refer to 3.1. Cyber Essentials or equivalent[3], is expected	
	Level 1	**Level 2 and Level 3**
Cyber Hygiene	Appropriate baseline security controls in place (refer to Level 0 Security Baseline requirements). Screen locking procedures. Backup and recovery plans. Implement, install, and maintain environmental controls.	*In addition:* Integrity verification tool to detect unauthorised changes to web-facing systems, critical software and firmware. Regular vulnerability management and/or penetration testing. Test and securely hold accessible current backups. Level 3 only – Automatically detect misconfigured or unauthorised system components.
Objective C: Detecting cyber security events The Supplier has capabilities which enable security defences to remain effective and detect cyber security events affecting, or with the potential to affect, Functions and protection of Data.		
Security Incidents and Events	Any compromise or suspected compromise to be managed internally; AWE to be informed. Detect malicious activity affecting the operation of business Function and protection of data	*In addition*: Engage Incident Response process when an incident is identified, including notification to AWE of any actual, near miss or suspected compromise of Official Assets; or a compromise to any IT system approved by AWE for work at OS.
Monitoring	Active security monitoring of networks and systems, to detect potential problems and track effectiveness of security measures. Security monitoring processes to cover; security events, frequency of monitoring, roles and responsibilities and an escalation matrix.	*In addition:* Suitable people, process and technology for monitoring, including specific tools and skills, shall be implemented as part of the monitoring activity. Monitor system security alerts and take action. Level 3 only– Continuous (24/7/365) monitoring of systems and networks.

Control	Level 0: Security Baseline requirements, refer to 3.1. Cyber Essentials or equivalent[3], is expected	
	Level 1	**Level 2 and Level 3**
Logs, Alerts and Management	Event logging shall be enabled for networks and systems to capture suitable data (logs) for legitimate auditing and review of activity, which should be retained for a suitable period and accessible upon approved request. Implement an appropriate audit record reduction and report. Integrate audit record review, triage, analysis, and reporting processes with organisational governance and incident management structure. Define examples of abnormal system behaviour to aid in detecting malicious activity. Monitor system security alerts and take action. Have measures to detect unauthorised assets and take action when detected.	*In addition:* Activity and event logs shall be stored securely with appropriate access Provide security incident evidence from monitoring tool to verify the reliability of alerts for triage. Implement measures to detect malicious activity affecting the operation of Functions and protection of Data.
Objective D: Minimising the impact of cyber security incidents The Supplier shall ensure capabilities exist to minimise the adverse impact of a cyber security incident on the operation of Functions and protection of Data, including the restoration of Functions and Data.		
Response and Recovery	Evidence of well-defined and tested; 1) incident management process 2) incident handling capability Implemented at an organisational level to ensure continuity in the event of a system or service failure with appropriate mitigation activities to contain or limit the impact of a cyber security incident.	*In addition:* Evidence of current; 1) incident response plan covering a range of scenarios 2) response and recovery capability to coordinate incident handling activities 3) business continuity risk assessments identifying risks, threats and impact of an incident, as well as controls and/or procedures to mitigate or remove risks and threats. Level 3 only – operation resilience for redundant networking and telecommunications equipment.
Testing, Exercises, Audits and Continuous Improvement	Evidence of suitable awareness of cyber security incident scenarios including an appreciation of suitable types of testing and exercising. Identify robust lessons learned function for suitable root cause analysis and processes to implement learning from experience. Evidence of suitable audit logging capability to capture denied capability communication on systems.	*In addition:* Identify the testing and exercising regime to validate incident response and recovery plans, based on simulated scenarios including data exfiltration tests.

3. Security Controls continued

3.9. Any AWE suppliers processing or storing AWE information on supplier IT (or other third-party IT) must be approved to do so by AWE, in accordance with the appropriate controls as set out in Table 2: Technical Control Requirements (see p9).

3.10. AWE will undertake suitable due diligence and supplier assurance of any supplier IT processing or storing personal or sensitive, including OFFICIAL-SENSITIVE (OS), information.

3.11. Typically, the security provenance AWE requires when a supplier presents a system that they would like to use to process AWE-related data are:

3.11.1. Significance/classification of data involved e.g. what data is at risk; aggregation, accumulation and/or association of information.

3.11.2. Security provenance of the system. Evidence of "Secure by Design" (see section 6) approach; other independent assurances.

3.11.3. Assurances can be achieved either by the Original Equipment Manufacturer (OEM) or the proposing supplier, e.g. conformance to NCSC or equivalent cloud security principles.

3.11.4. Visibility of access control mechanisms to maintain need to know principle in accordance with the core information security management principles of Confidentiality, Integrity and Availability (CIA); who can see what/how/from where.

3.11.5. Visibility of any offshore or third-party involvement, which could include hosting/support/app development.

3.12. AWE expects suppliers to have suitable controls in place to manage against standard IT security threats and potential attack.

3.13. AWE expects that where a supplier sub-contracts work (including outsourcing the management of IT systems) they will have carried out reasonable due diligence on those third parties and ensured that AWE security measures and controls as described in this document have been appropriately implemented. Suppliers may be required to provide visibility of where AWE-generated or related assets or material is at risk, e.g. by demonstrating Supply Chain Mapping of sub-contractors (and other lower tier third parties), as well as relevant cloud hosting, use of Artificial Intelligence/Machine Learning, collaboration environments, offshore exposure, and critical applications/SaaS solutions.

3.14. AWE expects that suppliers and sub-contractors maintain suitable levels of security controls by ongoing information security management assurance and/or maintaining certifications (e.g. annual renewal of Cyber Essentials Plus certification).

3.15. Suppliers undertaking work above OS will be subject to Facility Security Clearance (FSC) approval and their IT will have additional controls in place commensurate with the classification of work. See Secure by Design (section 6).

3.16. Further guidance is available from AWE.

4. Secure Connectivity

4.1. All suppliers (Direct and Sub-Contractors) required to receive personal or sensitive information, including OS, must be approved by AWE.

4.2. AWE will seek to establish secure connectivity arrangements with all Suppliers. Where personal or sensitive, including OS, data is being exchanged, data MUST be protected in transit (e.g. by encrypted email or media) to a level acceptable to AWE.

4.3. Exchange via email:

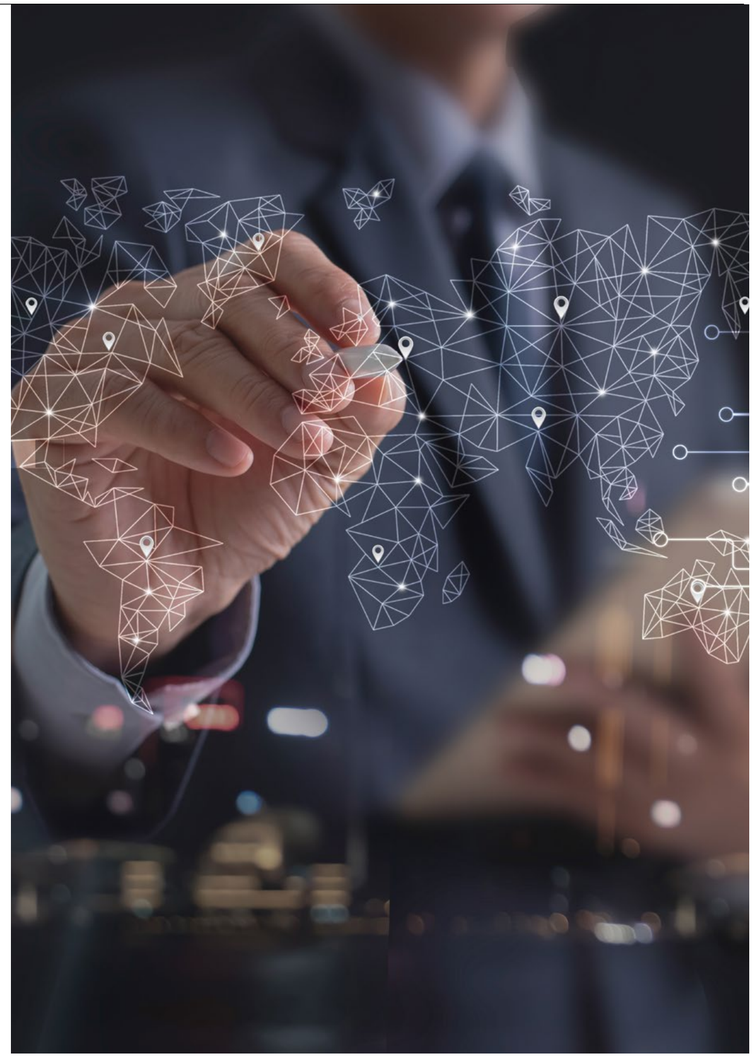
4.3.1. If there is a requirement to exchange emails at OS with AWE, the information must be protected in transit by enforced Transport Layer Security (TLS).[13] [14] It is AWE's policy to implement enforced TLS (at version 1.2 or later) between domains exchanging sensitive AWE information via email. We do not solely rely on opportunistic TLS. This policy extends throughout our supply chain so that; supplier to supplier (including sub-contractors) exchange of sensitive AWE information is permissible if the Suppliers have enforced TLS in place and that all Suppliers exchanging information are approved to do so by AWE. Sub-contractors must meet the requirements of working at OS (SP2/SP3), with any security aspects flowed down to them by AWE's direct (prime) supplier (i.e. carry out the appropriate checks; appropriate background checks, appropriate technical controls e.g. Cyber Essentials Plus, implement enforced TLS etc.).

4.3.2. It is best practice to implement additional email security controls[15], including anti-spoofing controls (DKIM, SPF, DMARC, PTR) and privacy controls (MTA-STS).

4.4. Exchange via file sharing applications:

4.4.1. The use of file sharing applications must be discussed with AWE prior to use for the exchange of AWE information.

4.5. Further guidance is available from AWE.



13 See: https://www.gov.uk/government/publications/email-security-standards/transport-layer-security-tls
14 See: https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data
15 See: https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing

5. Cloud Services and Artificial Intelligence

5.1. The use of Cloud Services for hosting AWE data must be approved by AWE, particularly where OS data will be stored and/or processed. Where AWE data is stored in a third-party Cloud system there is an increased risk to our information that must be understood, mitigated where necessary, and managed accordingly.

5.2. Use of Artificial Intelligence (AI) or Machine Learning (ML) to conduct AWE-related business must be approved by AWE. A key consideration in the assessment of AI/ML tools is whether AWE data is exposed to the public and used to train Large Language Models (LLM).

5.3. Where Cloud services are in use, suppliers should be satisfied that the Cloud environment has been designed, tested, and implemented in accordance with a recognised set of security standards e.g. the NCSC Cloud Security Principles[16]; the Center for Internet Security (CIS) Critical Security Controls; or the Open Web Application Security Project (OWASP) Top 10 Application Security Risks.

5.4. The Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) released five joint Cybersecurity Information Sheets[17] (CSIs) which recommend best practices to organisations and provide mitigations to improve the security of their Cloud environments. It is encouraged that organisations review the practices and implement such mitigations to help strengthen cloud security.

5.5. Cybersecurity Information Sheet:

5.5.1. Use Secure Cloud Identity and Access Management Practices

5.5.2. Use Secure Cloud Key Management Practices

5.5.3. Implement Network Segmentation and Encryption in Cloud Environments

5.5.4. Secure Data in the Cloud

5.5.5. Mitigate Risks from Managed Service Providers in Cloud Environments

5.6. 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[18].

5.7. Use of cloud based High Performance Computing (HPC) must be in accordance with above guidance and approval by AWE.

5.8. Further guidance is available from AWE.

16 https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles
17 https://www.cisa.gov/news-events/alerts/2024/03/07/cisa-and-nsa-release-cybersecurity-information-sheets-cloud-security-best-practices
18 https://www.ncsc.gov.uk/collection/cloud/using-cloud-services-securely/using-saas-securely

6. Secure by Design (SbD)

6.1. The Secure by Design approach (as per the Government Secure by Design Policy)[19] aims to increase the government's cyber resilience and improve data sharing between organisations.[20]

6.2. The UK Cabinet Office policy is that all government departments and arm's length bodies must be secure. Following a SbD approach will:[21]

6.2.1. Help create resilient capabilities and services

6.2.2. Make security everyone's responsibility

6.2.3. Improve trust and data sharing

6.3. The Ministry of Defence is implementing SbD in all top-level budgets and arm's length bodies. All capabilities and services that handle Defence data must follow SbD. This includes projects delivered by suppliers.

6.4. Any supplier system processing AWE classified material shall be subject to SbD assurance. This is to ensure systems processing AWE's most sensitive assets meet the recommended Government assurance requirements.

6.5. To align with good practice, any supplier systems in the Official Tier should align to SbD principles, in accordance with a suitable framework, i.e. NIST.

6.6. The implementation of SbD intends to enable a culture of proactive risk management and security consideration throughout a capability's lifecycle; by using cyber security principles, roles, processes, tools and techniques to secure systems and data; thereby ensuring protection from threats.

6.7. MOD Secure by Design Principles:[22]

6.7.1. Principle 1: Understand and Define Context. Understand the capability's overall context and how it will use and manage MOD data while achieving its primary business/operational outcome(s).

6.7.2. Principle 2: Plan the Security Activities. Establish security workstream of the capability, perform initial planning including assessment of cyber threat and potential risks while defining clear security requirements, validation and verification.

6.7.3. Principle 3: Implement Continuous Risk Management. Embed cyber security risk management into existing programme governance as a continuous process.

6.7.4. Principle 4: Define Security Controls. Define, architect and implement security control requirements to address risks identified. Reuse existing services and patterns where they exist.

6.7.5. Principle 5: Engage and Manage the Supply Chain. Understand the supply chain role and risks posed, including how to ensure they meet their responsibilities and implement good security.

6.7.6. Principle 6: Assure, Verify and Test. Work with security experts to gain security assurance, test and validate throughout the capability's lifecycle.

6.7.7. Principle 7: Enable Through Life Management. Ensure continuous security monitoring and improvements, including ongoing assurance requirements are enabled, met and disposed.

6.8. Further guidance is available from AWE.

19 https://www.security.gov.uk/policy-and-guidance/secure-by-design/policy/
20 https://www.security.gov.uk/policy-and-guidance/secure-by-design/about/
21 https://www.digital.mod.uk/policy-rules-standards-and-guidance/secure-by-design
22 https://assets.publishing.service.gov.uk/media/64bfb929d4051a00145a9289/ISN_2023-09_Secure_by_Design_Requirements.pdf

7. Recommended Resources

7.1. NCSC Cyber Security Services

7.1.1. Exercise in A Box (EiAB) [23]
EiAB is a free resource which helps organisations find out how resilient they are to cyber-attacks and practise their response.

7.1.2. Logging Made Easy (LME)[24]
LME is a no cost, open source platform that centralizes log collection, enhances threat detection, and enables real-time alerting, helping small to medium-sized organizations secure their infrastructure.

7.1.3. Early Warning/ My NCSC[25]
NCSC'S free service to organisations, designed to inform them of threats against their networks.

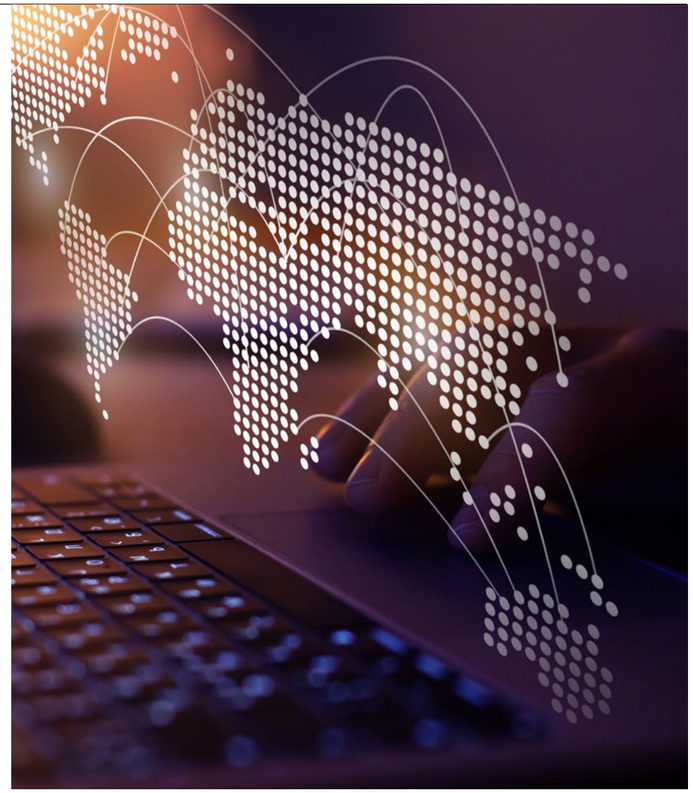
7.1.4. Vulnerability Disclosure Toolkit[26]
Security vulnerabilities are discovered all the time and people want to be able to report them directly to the organisation responsible. The NCSC's Vulnerability Disclosure Toolkit contains the essential components needed to set up a vulnerability disclosure process.

7.1.5. Email Security and Anti-Spoofing[27]
NCSC recommends the implementation of measures to prevent spoofing and secure email in transit in order to protect organisations and reduce the costs of service down-time due to email fraud. NCSC research shows these measures are not widely implemented to the recommended standards: this guidance provides all the information required to do so.[28]

7.1.6.[29] Phishing is when criminals use scam emails, text messages or phone calls to trick victims e.g. to click on a link, which may download a virus onto a computer, or steal bank details or other personal information.

7.1.7. Ransomware[30] Ransomware is a type of malware which prevents access to a device or to stored data, usually by surreptitiously encrypting file storage. A criminal group will then demand a ransom in exchange for decryption.

7.1.8. Certified Products and Services[31]
NCSC endorses a range of products and services that can help organisations protect themselves against cyber-attack.



23 See: https://www.ncsc.gov.uk/information/exercise-in-a-box
24 See: https://github.com/cisagov/LME
25 See: https://www.ncsc.gov.uk/section/active-cyber-defence/early-warning
26 See: https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit
27 See: https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing
28 Further guidance for securing government email can be found here: https://www.gov.uk/guidance/securing-government-email
29 See: https://www.ncsc.gov.uk/collection/phishing-scams
30 See: https://www.ncsc.gov.uk/ransomware/home
31 See: https://www.ncsc.gov.uk/section/products-services/all-products-services-categories

7. Recommended Resources continued

7.1.9. The NCSC's Cyber Advisor[32]

This scheme assures organisations to provide general cyber security advice and support to a broad range of UK organisations. The network of NCSC Assured Cyber Advisors provides tailored cyber security guidance, and practical hands-on help. The focus of the advice and support is on the implementation of the technical controls set out in Cyber Essentials and to improve the organisations' basic cyber security to avoid the disruption caused by some of the most common cyber-attacks.

7.1.10. Artificial Intelligence[33]

NCSC provides guidance on assessing intelligent tools for cyber security.

7.1.11. Machine Learning[34]

NCSC has introduced new machine learning security principles that define why the security of artificial intelligence (AI) and machine learning (ML) is so important.

32 See: https://www.ncsc.gov.uk/schemes/cyber-advisor
33 See: https://www.ncsc.gov.uk/collection/intelligent-security-tools
34 See: https://www.ncsc.gov.uk/blog-post/machine-learning-security-principles-updated

8. Further Guidance

The following sources of additional advice are recommended.

HM Government

Department for Business, Energy & Industrial Strategy

Ministry of Defence

HMG guidance on cyber security for businesses, and on Government Security Classifications. See:
https://www.gov.uk/government/cyber-security
https://www.gov.uk/government/publications/government-security-classifications

UK CYBER SECURITY COUNCIL

The UK Cyber Security Council is the self-regulatory body for the UK's cyber security profession.
It develops, promotes and stewards nationally recognised standards for cyber security in support of the UK Government's National Cyber Security Strategy to make the UK the safest place to live and work online.
See: https://www.ukcybersecuritycouncil.org.uk/

CERTIFICATION BODY CYBER ESSENTIALS

The Cyber Essentials scheme is explained at:
https://www.ncsc.gov.uk/cyberessentials/overview
https://ce-knowledge-hub.iasme.co.uk/

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/
https://www.ncsc.gov.uk/section/advice-guidance/all-topics

iasme

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/

Cyber Aware

The Cyber Advisor scheme assures organisations to provide general cyber security advice and support to a broad range of UK organisations.
See: https://www.ncsc.gov.uk/schemes/cyber-advisor

National Cyber Security Centre
a part of GCHQ

The NCSC's Cyber Action Plan is a free tailored Cyber Checklist. It helps organisations discover what they can do now to protect their business against cyber-attack and to see any gaps in preparation of the Cyber Essentials self-assessment.
See: https://www.ncsc.gov.uk/cyberaware

National Protective Security Authority

NPSA provides guidance on physical and personnel security, and on security awareness. It also publishes the Catalogue of Security Equipment.
See: https://www.npsa.gov.uk/building-protection
https://www.npsa.gov.uk/personnel-and-people-security
https://www.npsa.gov.uk/cse-categories

8. Further Guidance continued

NIST publishes US Government standards on information technology and cyber security. See: https://www.nist.gov/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/standard/27001 https://www.iso.org/standard/79612.html

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-us/

CIS provides guidance on cyber security, including the “18 CIS Critical Security 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/

8. Further Guidance continued

SANS

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

CyBOK

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

NIS2 DIRECTIVE

The EU NIS2 (Network and Information Security) Directive sets out the expectations for security of network and information systems within the EU.
See: https://nis2directive.eu/

9. Glossary

AES-256	Advanced Encryption Standard-256
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
AWE	Atomic Weapons Establishment
BPSS	Baseline Personnel Security Standard
CE/CE+	Cyber Essentials/Cyber Essentials Plus UK Government cyber security certification scheme
CIS	Center for Information Security
CISA	Cybersecurity and Infrastructure Agency
CISP	Cyber Security Information Sharing Partnership
CREST	Council of Registered Ethical Security Testers
CSI	Cyber Security Information Sheet
CyBOK	Cyber Security Body of Knowledge
DISA	Defence Industry Security Association
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication, Reporting & Conformance
EiAB	Exercise in A Box
FSC	Facility Security Clearance (formerly List X)
GDPR	General Data Protection Regulation
IASME	Information Assurance for Small and Medium Enterprises
IPSA	Industry Personnel Security Assurance
ISF	Information Security Forum
ISO	International Standards Organisation
IT	Information Technology
LME	Logging Made Easy
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MOD	Ministry of Defence
MTA-STS	Mail Transfer Agent Strict Transport Security
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NIS2	Network and Information Security Directive;
NPSA	National Protective Security Authority (formerly CPNI; Centre for the Protection of National Infrastructure)
NSV	National Security Vetting
NTP	Network Time Protocol
O	OFFICIAL
OEM	Original Equipment Manufacturer
OS	OFFICAL-SENSITIVE
OWASP	Open Worldwide Application Security Project
PC	Personal Computer
PII	Personally Identifiable Information
PTR	(DNS) Pointer Record
SaaS	Software as a Service
SbD	Secure by Design
SDLC	Software Development LifeCycle
SOC2	System and Organisation Controls audit relevant to security, availability, processing integrity, confidentiality, or privacy
SPF	Sender Policy Framework
TLS	Transport Layer Security
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WASP	Web Application Security Project

All links to external websites and resources are accurate at the time of publication.

NUCLEAR SECURITY TECHNOLOGIES

End of document