AWE NUCLEAR SECURITY TECHNOLOGIES

Supply Chain Security

Security Requirements for the AWE Supply Chain

Issue 1: September 2025

Introduction

AWE is responsible for the design, manufacture, maintenance and development of the United Kingdom's sovereign warheads - a critical part of the UK's Independent Nuclear Deterrent - and protects the United Kingdom through nuclear science and technology.

We know that we cannot do this alone, and so we put significant effort into ensuring how we and our Supply Chain partners can work together safely and securely.

This document replaces the following:

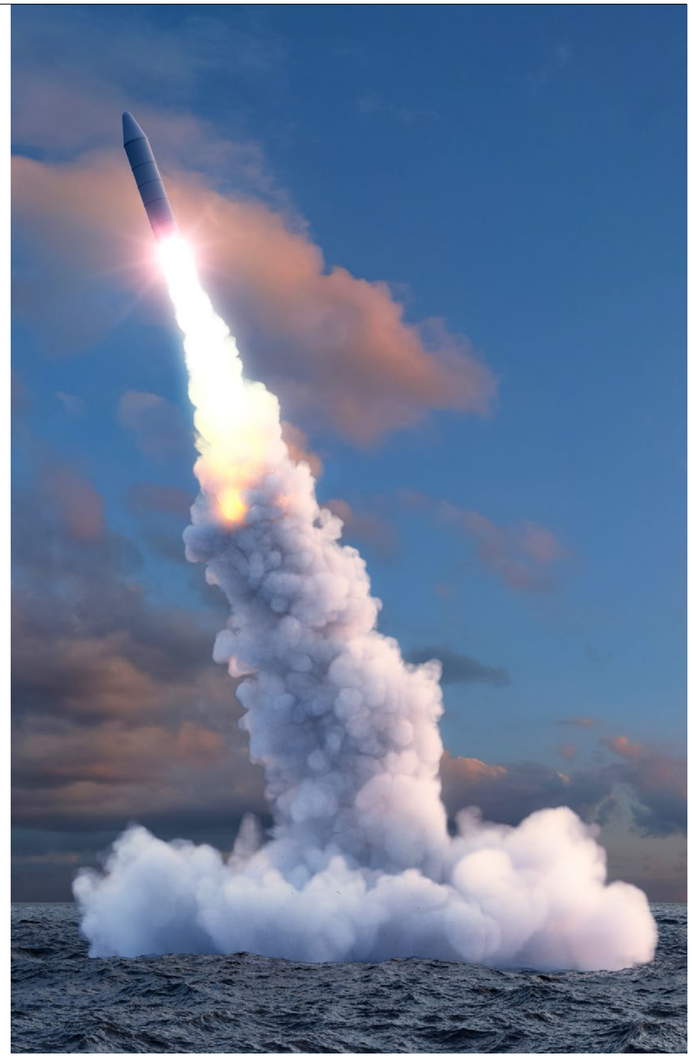
In this document we set out AWE's security requirements so that our Supply Chain partners understand how to protect and handle Official Assets in respect of information (cyber) security as well as physical, personnel and procedural security arrangements.

The AWE Supply Chain

Our security requirements extend beyond just those companies who are in direct (prime) contract with us. It applies wherever there is risk to AWE or to Official Assets, which will cover:

- direct (prime) Suppliers to AWE
- sub-contractors[1] to our direct (prime) Suppliers
- specialist IT and/or 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 which support AWE projects and/or our capabilities

1 The term "sub-contractor" throughout this document includes any company being sub-contracted through one of our direct Suppliers or any subsequent lower tier suppliers; the extent of AWE risk and risk management requirements will be determined on a case-by-case basis.



Introduction

Official Assets

Official Assets means any information, document, article and/or material provided to a Supplier by AWE or any associated Supplier; or procured from, or created by our Supply Chain in support of any AWE requirement, where, for the purpose of protecting the safety or interests of the United Kingdom, access to said information, document, article and/or material is restricted in any way; or it is reasonable to expect such access would be restricted in any way.

Commercial documentation (purchase orders, Terms and Conditions etc.) are not normally considered Official Assets in this context.

The Official Tier

OFFICIAL is one of three Government Security Classifications.[2] The Official Tier is where AWE conducts day-to-day business. It is also the Tier where the AWE Supply Chain conducts a large amount of project and supporting work.

Some Official Tier information will be of a more sensitive nature and be identified as requiring additional technical and procedural controls to reinforce the Need-To-Know (NTK) principle: it may bear an OFFICIAL-SENSITIVE (OS) security marking; or be identified by specific handling instructions or Security Conditions. OS is **not** a separate classification tier.

Classified Projects

Suppliers engaged on projects involving *Classified Material* (information/material classified above the Official Tier) must be approved to do so under *FSC Arrangements*.

Facility Security Clearance (FSC) Arrangements

It is essential that prospective and current FSC suppliers understand the security arrangements that are required to be in place for engagements at this level. Under FSC Arrangements, Suppliers will be subject to additional controls, approvals, and assurance oversight. Any IT systems used to process data at these levels will be subject to a formal assurance programme. Please contact fsc@awe.co.uk for further guidance.

Official Secrets Act & National Security Act

The provisions of the Official Secrets Act 1989[3] and the National Security Act 2023[4] apply to any AWE requirement.

Our Suppliers will understand the need to protect any Official Assets they may receive or generate and not to disclose or provide access to those Assets unless authorised to do so by AWE.

Security Aspects Letters (SAL)

For all engagements at OS and for Classified Projects AWE will issue a SAL, which contractually imposes the relevant Security Conditions and/or associated limitations or security requirements.

2 The three classification tiers are OFFICIAL, SECRET and TOP SECRET. They are used to correctly identify Official Assets by use of security labels, and to reflect the need to appropriately protect and handle Official Assets classified in the upper tiers by use of proportionate technical, physical and supporting procedural controls. The term Classified Material in this document is meant as Official Assets classified at SECRET or TOP SECRET. See: Government Security Classifications Policy (HTML) - GOV.UK - https://www.gov.uk/government/publications/government-security-classifications/government-security-classifications-policy-html

3 Official Secrets Act 1989 - https://www.legislation.gov.uk/ukpga/1989/6/contents

4 National Security Act 2023 - https://www.legislation.gov.uk/ukpga/2023/32/contents

Offshore Exposure

We recognise the benefits that come from being able to source materials, goods and services from non-UK companies, and those that operate in a global market.

Where there is a requirement for work being offshored, this must be approved by AWE. This includes the delivery (by the Supplier, any associated third-party or any sub-contractors) of any work undertaken for, or any access to Official Assets, by individuals or entities based outside the UK. Suppliers will understand that due to the nature of our work, there will be some jurisdictions where offshoring will not be possible, though the Official Tier is operated within a realistic risk appetite and we will be amenable to considering appropriate offshoring.

AWE retains the discretion to deny any offshore component or delivery of any aspect of any requirement, which in the reasonable opinion of AWE represents a risk to the national security of the United Kingdom.

Foreign Ownership, Control or Influence

All AWE suppliers are required to identify and to make AWE aware of any entity involved in any aspect of the delivery of any requirement which is subject to Foreign Ownership, Control or Influence (FOCI)[5].

FOCI status will be considered at the outset of any engagement.

AWE retains the discretion to exclude the delivery of any aspect of any requirement by entities which have any direct or indirect FOCI connection to any person or entity subject to any form of sanctions imposed by the UK, EU or US governments; or which in the reasonable opinion of AWE represents a risk to the national security of the United Kingdom.

If there is any change to either offshore exposure or FOCI status in respect of any of our Suppliers, associated third parties or sub-contractors, AWE should be informed at the earliest opportunity.

Sourcing of Materials and Equipment

There may be security concerns which arise from materials and/or equipment which originates from overseas sources.

Further guidance is available from AWE.

Trade and Export Controls

Should any Official Assets be subject to Trade and Export controls AWE must be notified in order for appropriate approvals to be given.

Further guidance is available from AWE.

5 An entity is considered to be subject to FOCI if it is or may be, directly or indirectly, owned or controlled by a Foreign Person; Foreign Company; or Foreign Entity; or if any Foreign Person, Foreign Company or Foreign Entity has any ability, directly or indirectly, to direct or decide matters affecting the management or operations of the entity including but not limited to acting in a manner which may result in unauthorised access to Official Assets or may otherwise adversely affect the delivery of any requirement, or represent a risk to the interests of the United Kingdom. Foreign Person is any individual other than a sole British Citizen; Foreign Company means a company that is not incorporated and registered in the UK. Foreign Entity means any legal entity (other than a Foreign Person or Foreign Company) that is not established or registered in the UK.

Procurement Categories

Our Suppliers and associated third parties and sub-contractors, will be expected to meet and maintain a range of proportionate security measures.[6] These measures, covering cyber, physical, personnel and procedural security arrangements, will be specified as a Security Profile and will be determined by AWE based on the nature and classification of the requirement (a Procurement Category).

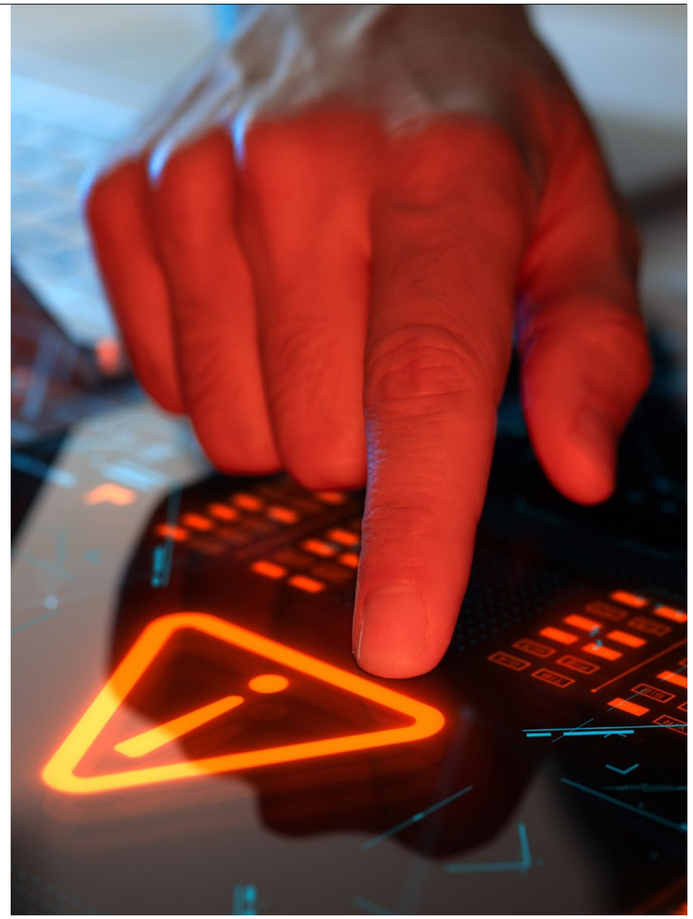
Procurement Categories

PC1 Commodity goods (i.e. COTS items) and/or services not associated with any operational or sensitive capability, and where no Official Assets are at risk.

PC2 Goods and/or services where only OFFICIAL Assets are at risk. This category will also include non-sensitive consultancy services, or the provision of limited modified items which support any operational or sensitive capability.

PC3 Goods and/or services where OFFICIAL-SENSITIVE Assets are at risk, or where bespoke items or business services where aggregated data is at risk.

PC4 Classified goods and/or services above the Official Tier can only be delivered by companies which have attained FSC status.

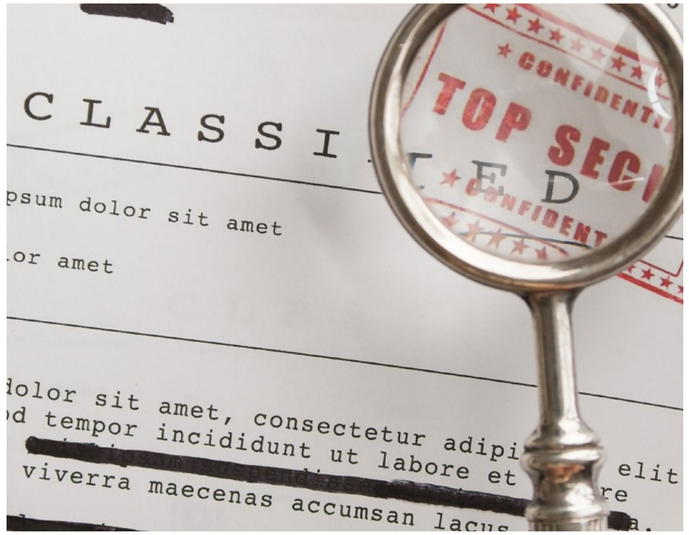


6 See Supply Chain Security:
https://www.awe.co.uk/our-supply-chain/our-suppliers/supplier-assurance/

Security Profiles

Security Profile

There are four Security Profiles (SP0-SP3) with associated minimum control measures. They are set out in the Technical Supplement[7] to this document as are additional security requirements for Cloud Environments and for FSC arrangements.



7 See https://www.awe.co.uk/our-supply-chain/our-suppliers/supplier-assurance/

Security Profiles

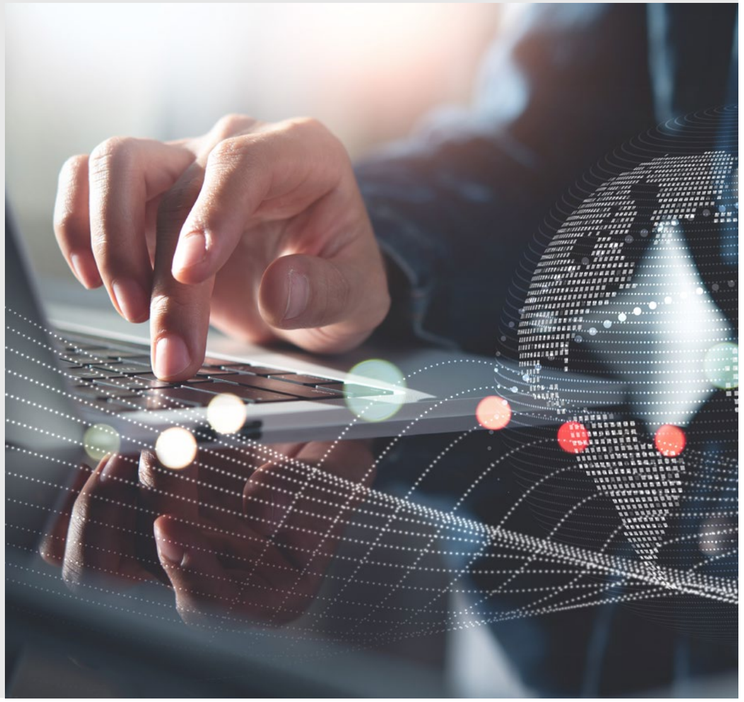
SP0 AWE's security baseline, which we expect all our suppliers to be able to meet. This is applicable to those requirements which present a negligible risk to AWE, our sites and facilities, which do not impact any of our operational capabilities and where no Official Assets are at risk. The associated minimum controls reflect commercial good practice.

SP1 Applicable to those Suppliers who deliver requirements which present a very low risk to AWE, the secure operation of our sites and facilities and/or support to our operational capabilities. This is the default profile for the protection of Official Assets classified at OFFICIAL e.g. for goods and/or services beyond solely Commercial Off the Shelf (COTS) items.

SP2 Applicable to those Suppliers who deliver requirements which present a low to medium risk to AWE, the secure operation of our sites and facilities and/or are involved in our operational capabilities. This is the default profile for the protection of OS Assets which we may need to release to our Suppliers, or for goods and/or services attracting additional handling requirements commensurate with the OS security label.

SP3 Applicable to those requirements where significant amounts of AWE-related Assets are at risk e.g. aggregated Personally Identifiable Information (PII) or other sensitive data.

To meet the controls of a Security Profile, the preceding profile controls must also be met.



Supplier Assurance and Due Diligence

We understand that many of our suppliers will need to outsource or sub-contract elements of their work for us. 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 the appropriate control measures have been implemented.

Suppliers are required to provide visibility of where Official Assets are at risk e.g. by demonstrating Supply Chain Mapping of sub-contractors (and other lower tier third parties) as well as relevant cloud hosting, collaborative environments and offshore exposure.

Our standard contractual terms require outsourcing and sub-contracting to be visible to us and we expect that appropriate handling instructions will be flowed down.

Prospective Suppliers

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 discretion and commercial sensitivity.

IT Support Companies

We understand and accept that our supply chain may rely on a third party for the provision, operation, management and/or administration of their IT estate. We expect any IT support company to be operating to at least the same Security 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 IT support companies will be expected to meet Security Profile 2 (SP2) and/or be able to demonstrate acceptable independent assurance of their IT security arrangements.

Cloud Environments

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.

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 be subject to AWE approval.

8 Lightweight approach to cloud security: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/lightweight-approach-to-cloud-security

Supplier Assurance and Due Diligence

Use of Artificial Intelligence (AI) and Machine Learning (ML)

Use of AI or ML to conduct AWE-related business must be approved by 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.

9 Bring your own device (BYOD) - NCSC.GOV.UK
https://www.ncsc.gov.uk/collection/mobile-device-guidance/bring-your-own-device

Right to Audit and Security Assessments

AWE will conduct security assessments of its supply chain at various stages:
- during the onboarding assessment
- periodic reassessment of existing suppliers
- periodic contract renewal or change of contract point

Suppliers will be asked to submit a conformance statement and/or evidence of up-to-date 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 there is a higher degree of risk to our operations and/or our capability
- where Personally Identifiable Information (PII) and/or other sensitive data is at risk
- where Official Assets are at risk offshore
- when novel solutions are proposed
- to explore FOCI concerns

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. Further assurance activity may take place based on the level of risk and AWE's confidence in the Supplier's ability to maintain and operate acceptable security arrangements.

Security Incidents

Suppliers are required to inform us, at the earliest opportunity, if there have been any actual, near-miss or suspected compromise of Official Assets. This includes the failure or degradation of a security control which is designed to protect those assets; or a compromise to any IT system which AWE has approved to process, store or forward PII and/or information at OS.

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

Personnel and Physical Security

We expect all companies within our Supply Chain to operate an appropriate employment regime, which should include pre-employment and recruitment checks, and in-service controls. These will typically include personal and management responsibility for the implementation of and adherence to security procedures, supported and reinforced through training and company policies.

All those persons directly engaged on AWE work – with access to Official Assets – should meet a minimum recruitment control of the minimum Baseline Personnel Security Standard (BPSS)[10] or an equivalent[11] acceptable to AWE.

For those who require access to AWE sites, and/or have to work with Classified Material additional security clearances under National Security Vetting (NSV) arrangements are required.

Nationality Requirements

In order to manage any potential risks to the national security interests of the United Kingdom, we have to apply some limitations on the nationalities of those persons who are directly engaged on AWE work and have access to Official Assets.

Guidance should be sought from AWE in respect of any person who is not a sole British Citizen.

Those who require access to AWE sites, and/or have to work with Classified Material, must be either a sole British Citizen or a British/Dual National, where the second nationality is one acceptable to AWE.

Further guidance is available from AWE.

Physical Security

Appropriate control mechanisms should be implemented to deliver a layered and balanced physically secure working environment to protect against loss, theft and/or compromise of Official Assets by forcible or surreptitious attack.

These need to include:
- establishment of an appropriate control environment
- accounting for Official Assets
- effective barriers
- access controls
- detection of actual or attempted compromise
- regular testing of effectiveness of physical security arrangements

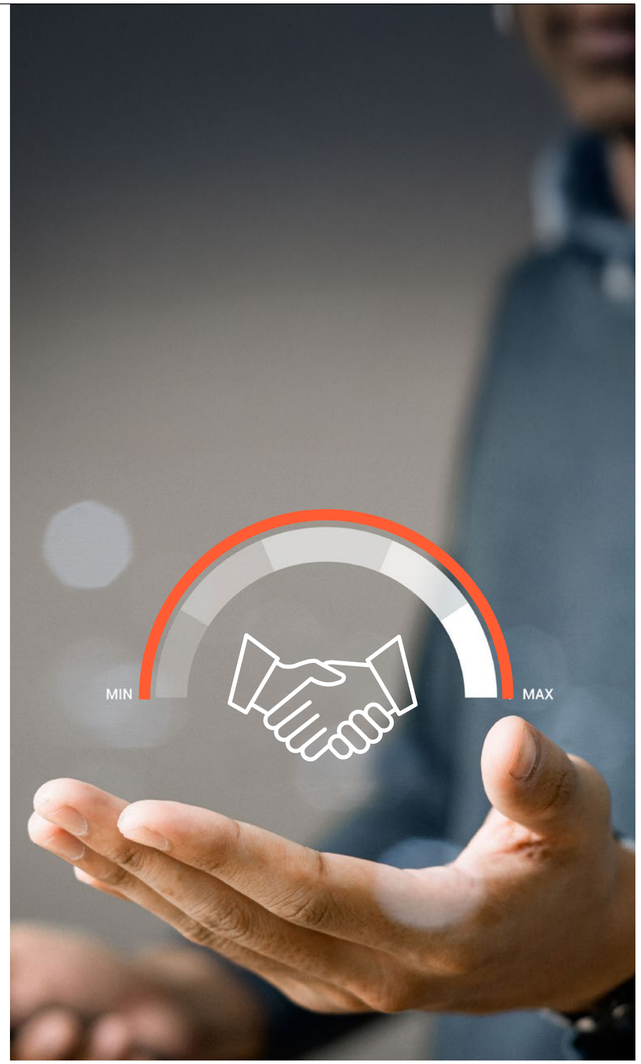
Work in the Official Tier may be conducted in business premises of a Supplier, any associated third-party or any sub-contractors; including under approved remote working arrangements. Offshore working requires prior AWE approval.

10 See: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
11 BPSS equivalence includes recruitment controls covering: Identity Verification and Immigration (right to work) status: Employment History (3 years minimum): and a Criminal Record Check (unspent convitions).

Glossary

AI	Artificial Intelligence
AWE	Atomic Weapons Establishment
BPSS	Baseline Personnel Security Standard
BYOD	Bring Your Own Device
Classified Material	Information/material classified above the Official Tier
COTS	Commercial Off The Shelf
EU	European Union
FOCI	Foreign Ownership, Control or Influence
Foreign Company	A company that is not incorporated and registered in the UK
Foreign Entity	Any legal entity (other than a Foreign Person or Foreign Company) that is not established or registered in the UK
Foreign Person	Any individual other than a sole British Citizen
FSC	Facility Security Clearance
IT	Information Technology
ML	Machine Learning
MOD	Ministry of Defence
NCSC	National Cyber Security Centre
NSV	National Security Vetting
NTK	Need-to-Know
O	OFFICIAL
Official Assets	Any information, document, article and/or material provided to a Supplier, where, for the purpose of protecting the safety or interests of the United Kingdom, access to said information, document, article and/or material is restricted in any way
OS	OFFICIAL-SENSITIVE
PII	Personally Identifiable Information
SaaS	Software as a Service
SAL	Security Aspects Letter
Security Conditions	Additional controls and risk treatment measures specified within a Security Aspects Letter (SAL) and applied under contractual arrangements
UK	United Kingdom
US	United States

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



NUCLEAR SECURITY TECHNOLOGIES

End of document