Department for Transport

Department for Business, Energy & Industrial Strategy

UK SPACE AGENCY

UK Civil Aviation Authority

Guidance on security matters for applicants and licensees

CAP 2217

Published by the Civil Aviation Authority, 2021

Civil Aviation Authority
Aviation House
Beehive Ring Road
Crawley
West Sussex
RH6 0YR

29 July 2021

Any enquiries regarding this publication should be sent to us at: SpaceTeam@dft.gov.uk

Contents

Section 1: Overview of the Guidance

Introduction

1.1 The Space Industry Act 2018 (the Act) regulates all spaceflight activities carried out in the United Kingdom, and associated activities.

1.2 The Act requires any person or organisation wishing to:

- launch a launch vehicle from the UK
- return a launch vehicle launched elsewhere than the UK to the UK landmass or the UK's territorial waters
- operate a satellite from the UK
- conduct sub-orbital activities from the UK
- operate a spaceport in the UK, or
- provide range control services from the UK

to obtain the relevant licence.

1.3 It is supported by The Space Industry Regulations 2021 (the Regulations), that set out in more detail the requirements for each licence, and the Regulator's Licensing Rules, which specify which application form to use to apply for a licence and what information the regulator will require in support of an application.

1.4 There is then a series of guidance documents designed to help explain how to comply with the Act and the Regulations. This document is one of the guidance documents.

With the coming into force of section 1(3) of the Act, the Outer Space Act 1986 no longer applies to space activities carried on in the United Kingdom, and accordingly the Outer Space Act 1986 does not apply to a person or organisation wishing to carry out spaceflight activities or operate a spaceport in the United Kingdom. The Outer Space Act 1986 **will** continue to regulate the following activities carried out overseas by UK entities: the procurement of the overseas launch of a space object, where the procurement takes place in the UK; the operation of a satellite in orbit from an overseas facility by a UK entity. Extant licences granted under the Outer Space Act 1986 for the carrying out of space activities from within the UK will continue to be governed under that regime. Where an application for a licence has been made under the Outer Space Act 1986, it will be assessed under that Act and – where successful – will result in the award of a licence under the Outer Space Act 1986.

What is the purpose of this guidance document?

1.5 This document sets out the fundamental security principles and requirements for all licence types, where applicable, under the Act. It does not provide guidance for the security of any state sponsored military spaceflight operations from a military launch site.

1.6 Further security restricted information will be made available by the regulator where this is necessary to progress a proposed application, or where an application for a licence has been granted and further security guidance is required by the licensee. Such guidance will be provided by the regulator to a nominated individual or individuals; these individuals may need to hold a certain level of security clearance, in accordance with the security classification of the information.

Who is this guidance for?

1.7 This guidance is for applicants and licensees wishing to carry out commercial spaceflight activities and associated activities in the UK, to help them understand the necessary security requirements relating to the physical, personnel and cyber security of space sites[1] and operations. It also covers facilities, equipment, spacecraft, carrier aircraft, other vehicles, payloads, cargo, and supplies at space sites.

Using this guidance

1.8 This guidance document should be read in conjunction with the Act, the Regulations and the Regulator's Licensing Rules. Where appropriate, the guidance contains links to each of these.

1.9 This guidance is designed to provide licensees and licence applicants with general information on security principles and methods that will help them comply with any applicable regulatory requirements for security required under the Act and the Regulations made under it.

1.10 Security regulations are cross-cutting and will apply to all licence types. However, not every regulation will apply to each type of licence. For example, regulation 177 (security controls for supplies) of the Space Industry Regulations 2021 would only apply to a spaceport licence and not to an orbital operator licence.

1.11 This guidance is not intended to be exhaustive; it is designed to assist licensees in developing security procedures that are both proportionate and appropriate to the activity being undertaken and deemed to be compliant by the regulator. For example, security measures which would be appropriate to launch a high-altitude balloon from a field would not necessarily be the same as the measures required to launch a rocket from a purpose-built spaceport.

1.12 If applicants have any queries, they are encouraged to contact the regulator, to seek clarification or gain further information.

The regulator

1.13 The Civil Aviation Authority (CAA) will perform the functions of the regulator under the Act. It is referred to in this guidance as 'the regulator'. Under section 2 of the Act, the regulator must carry out its functions relating to spaceflight activities with a view to securing the health and safety of members of the public and the safety of their property. This duty has primacy over the other matters that the regulator must take into account in exercising its functions.

1.14 In performing its functions, the regulator will need at times to review confidential and commercially sensitive information. The regulator already has robust security processes in place that will ensure all the information sent in relation to applications, and monitoring ongoing licensed activities, is handled and protected appropriately. For more details on the regulator's security processes and systems, please contact the regulator.

1.15 Section 25 of the Act sets out that the regulator may provide advice and assistance on security matters to a licensee or an associated company of a licensee, when requested. All applicants / licensees may request further, specific advice from the regulator about security matters relating to any relevant activity, service,

[1] Space site has the meaning given in paragraph 5(3) of Schedule 4 of the Act. See paragraph 1.27 and footnote 3 of this guidance for further information as to how it relates to a sea launch.

site, facility or other matter under section 23 of the Act. However, it should be noted that section 25(7) allows the regulator to recover the costs of providing that advice, from the recipient.

Contacting the regulator
The regulator can be contacted by email to commercialspaceflight@caa.co.uk**.** The regulator welcomes and encourages ongoing contact from prospective applicants before they submit an application for a licence. This can be from the earliest stages of considering whether to apply for a licence.

Key terms

1.16 The Act regulates:

- space activities
- sub-orbital activities
- associated activities

that are carried out in the UK.

1.17 As set out in section 1 of the Act, "space activity" means

(a) launching or procuring the launch or the return to earth of a space object or of an aircraft carrying a space object
(b) operating a space object, or
(c) any activity in outer space

1.18 "A space object" includes the component parts of a space object, its launch vehicle and the component parts of that.

1.19 "Sub-orbital activity" means launching, procuring the launch of, operating or procuring the return to earth of:

(a) a rocket or other craft that is capable of operating above the stratosphere
(b) a balloon that is capable of reaching the stratosphere carrying crew or passengers, or
(c) an aircraft carrying such a craft

but does not include space activity. By way of clarification, the regulator will use the International Standard Atmosphere (47km) as the stratopause (i.e. the upper limit of the stratosphere) for the purposes of determining whether an activity is 'sub-orbital'.

1.20 Space activities and sub-orbital activities are referred to in the Act as "spaceflight activities".

1.21 "Spacecraft" means a space object, a rocket or other craft that is capable of operating above the stratosphere or a balloon that is capable of reaching the stratosphere carrying crew or passengers, that is used for spaceflight activities. It includes satellites.

1.22 "Launch" is defined in the Act as including causing a craft to take off (or releasing a balloon).

1.23 Regulation 2 of the Space Industry Regulations defines a launch vehicle, other than in references to a "US launch vehicle", as:

"(a) a craft to which section 1(5) of the Act applies and the component parts of that craft, or
(b) a space object which is a vehicle and the component parts of that vehicle,

that is used for the purpose of the proposed spaceflight activities or the operator's spaceflight activities, as applicable, but does not include a payload carried by the launch vehicle;"

1.24 The "craft to which section 1(5) of the Act applies" referred to in part (a) of this definition are:

- a rocket or other craft that is capable of operating above the stratosphere
- a balloon that is capable of reaching the stratosphere carrying crew or passengers

1.25 Part (b) of the definition covers vehicles that are capable of reaching orbit, such as those used to place a satellite payload in orbit. As explained below, the operator of any satellite carried on board a launch vehicle does not require their own launch operator licence but does require an orbital operator licence.

1.26 Associated activities include the operation of spaceports and range control functions.

1.27 Under the Act, any site from which a spacecraft or carrier aircraft is intended to launch is considered a spaceport and must be licensed. A site at which controlled and planned landings of spacecraft are to take place is also a spaceport and must be licensed.

1.28 Range control services are defined in section 6 of the Act as:

"(a) identifying an appropriate range for particular spaceflight activities;
(b) co-ordinating arrangements for the activation and operation of the range;
(c) obtaining all necessary information for identifying the range and for co-ordinating its activation and operation;
(d) ensuring that notifications are issued for the protection of persons who might be put at risk by spacecraft or carrier aircraft within the range or in the vicinity of it;
(e) monitoring the range, and the spacecraft or carrier aircraft for which it is provided, to ascertain
(i) whether the restrictions or exclusions to which the range is subject are complied with;
(ii) whether planned trajectories are adhered to;
(f) communicating any failure to comply with those restrictions or exclusions, or to adhere to those trajectories, for the purpose of enabling any appropriate actions to be taken in response;
(g) any prescribed services provided for the purposes of, or in connection with, services within any of paragraphs (a) to (f)."

1.29 Under section 13(1) of the Act, the regulator has the power to include conditions in an operator licence (launch operator licence, return operator licence and orbital operator licence), spaceport licence and a range control licence. Licensees must comply with those conditions. Schedule 1 of the Act includes a list of examples of conditions, but this is not exhaustive, and the actual conditions included in a licence will vary depending on the operation planned and the type of licence issued. When deciding what conditions to include in a licence, the regulator must consult the public bodies, including the Health and Safety Executive, listed in section 13(6) of the Act. Whenever the guidance refers to the regulator imposing conditions (other than a condition which the regulator is required to impose via the Regulations under section 13(3)), the obligation to consult these bodies applies.

Carrying out spaceflight activities at sea

1.30 If a person is proposing to launch or carry out other spaceflight activities from UK territorial waters or from a UK flagged ship elsewhere, the Act and Regulations will regulate the activities. Where appropriate, regulations which refer to land also apply to spaceflight activities from a ship – for example, where a regulation refers to a "place" or "other place" from which activities take place, in addition to activities from land. If a person is proposing to launch or carry out other spaceflight activities from a foreign flagged

ship outside UK territorial waters and is a British national, UK body corporate or Scottish firm, the Outer Space Act 1986 regulates these activities.

1.31 Sea launch and other sea activities are a complex area; organisations wishing to conduct sea launches are advised to contact the regulator before applying for a licence. Further information on this can be found in section 2 of the guidance document Applying for a licence under the Space Industry Act 2018.

Requirements and expectations

1.32 Where the guidance uses the term "must", this refers to a requirement in or under the Act. If applicants / licensees fail to meet that requirement, it could result in the licence not being granted or being revoked or suspended. Where it is stated that "the regulator expects" applicants to do something, this describes a preferred approach; however, it is not a legal requirement to comply with the regulator's expectations.

Types of licence

1.33 The Act refers to three types of licences that can be awarded:

- operator licence
- spaceport licence
- range control licence

1.34 Following the publication of the Act, it was agreed that there should be different licensing requirements for different types of operators. For example, some organisations that would want to operate space objects (such as satellites or research vehicles) would not have a launch capability, and instead would wish to procure such capability and then operate the object once it reached orbit. While these organisations clearly do not need a licence to operate a launch vehicle, they are still required to obtain an operator licence to operate their object in space. Reflecting the various circumstances, there are now five licences available:

- **Launch operator licence**: means an operator licence within section 3 of the Act which authorises a person or organisation to carry out spaceflight activities that include launching a launch vehicle or launching a carrier aircraft and a launch vehicle. This is the type of licence needed if a person or organisation wants to launch a launch vehicle or use a carrier aircraft to assist with a launch of a launch vehicle. A person or organisation holding a launch operator licence is referred to as a spaceflight operator,[2] or in some circumstances, launch operator licensee. If a launch operator licensee wishes to return a launch vehicle launched from the UK or the UK's territorial waters to land in the UK, it can apply to do so under the launch operator licence and does not need to apply for a separate return operator licence.

- **Return operator licence:** means an operator licence within section 3 of the Act which is not a launch operator licence and which authorises a person or organisation to operate a launch vehicle, launched into orbit from elsewhere than the United Kingdom, in order to cause that vehicle to land in the United Kingdom. This is the type of licence needed if a person or organisation wants to return a launch vehicle, launched elsewhere than the United Kingdom, to land in the UK or within

[2] The term spaceflight operator is used in the Regulations to refer to both the holder of a launch operator licence and the holder of a return operator licence. Any references to spaceflight operator in the Regulations or guidance encompass both licence types, so any requirements for spaceflight operators are applicable to both launch operator licensees and return operator licensees. Where a requirement only applies to either a launch operator licensee or return operator licensee, this is clearly stated.

the UK's territorial waters. A person or organisation holding a return operator licence is referred to as a spaceflight operator,[1] or in some circumstances, return operator licensee.

- **Orbital operator licence**: means an operator licence which authorises a person or organisation to procure the launch of a space object into orbit, operate a space object in orbit or conduct other activity in outer space. The most common examples of activities that would be licensed under an orbital operator licence are the procurement of a satellite launch and the operation of a satellite. However, the licence may also cover any other activity in outer space, and is not limited to activities in Earth's orbit. For example, an orbital operator licence would be needed for missions in lunar orbit, lunar surface missions, or deep space probes. A person or organisation holding an orbital operator licence is referred to as an orbital operator licensee.

- **Spaceport licence**: means a licence granted under section 3 of the Act authorising a person or organisation to operate a spaceport (i.e. a site from which spacecraft or carrier aircraft can be launched or a site at which controlled and planned landings of spacecraft can take place[3]). Spaceports can be licensed for vertical or horizontal launches (or potentially both). A horizontal spaceport must be located at an aerodrome that is already CAA licensed or certified and National Aviation Security Programme (NASP) directed. A person or organisation holding a spaceport licence is referred to as a spaceport licensee.

- **Range control licence**: means a licence granted under section 7 of the Act authorising a person or organisation to carry out range control services in relation to spaceflight activities. That includes identifying an appropriate range; coordinating the use of a range; issuing protective notifications and monitoring the range. A person or organisation holding a range control licence is referred to as a range control licensee.

Examples of offences and enforcement directions under the Act

1.35 Under section 3 of the Act, it is an offence to carry out spaceflight activities or operate a spaceport in the UK without the required licence. It is also an offence to make a false statement for the purpose of obtaining an operator licence or a spaceport licence. A person who commits an offence under this section of the Act may be liable to a fine or imprisonment for a term not exceeding 2 years, or both.

1.36 Under section 7 of the Act, it is an offence for range control services to be provided by anyone other than the Secretary of State, or a person or organisation authorised to provide them by a range control licence. It is also an offence for a person to make a false statement for the purpose of obtaining a range control licence. A person who commits an offence under this section of the Act may be liable to a fine or imprisonment for a term not exceeding 2 years, or both.

1.37 Under section 13 of the Act, the regulator can grant a licence subject to conditions it thinks appropriate or must include a licence condition if required to do so by a regulation (see regulations 9(5) and 10(2)). When a condition is imposed, it is an offence for a licensee to fail to comply with that condition.

1.38 Under section 17 of the Act, it is an offence for a spaceflight operator to allow any person to take part in spaceflight activities without them having given their informed consent and fulfilling the age and mental capacity criteria referred to in Part 12 of the Regulations. Under

[3] Ships used for sea launch or landing are not "sites" and are therefore not spaceports for the purposes of section 3 of the Act and so do not need a spaceport licence. However, certain types of installations at sea may be regarded as a "site" and so come within the definition. A person who wants to launch from, or land at, an installation at sea should contact the regulator to find out whether the installation they propose to use requires a spaceport licence.

section 18 of the Act, it is an offence a licensee to allow any unqualified individual to take part in activities authorised by the licence or work in a specified role.

1.39 Under regulation 194 of the Regulations, it is an offence for the person who owns or is in possession of US technology not to ensure that access to that technology is controlled by a person authorised to do so by the US Government.

1.40 Under section 27 of the Act, the regulator can also issue directions that enable effective enforcement action to be taken, where it appears to the regulator that a person is carrying out spaceflight activities or associated activities without a licence, in contravention of licence conditions or in contravention of the Act or rules made under it.

1.41 Under section 27(2), "the regulator may give any directions to that person that appear necessary to be in the interests of safety or for the purposes of securing compliance with–

(a) the conditions of a licence,
(b) provisions contained in or made under this Act, or
(c) the international obligations of the United Kingdom."

1.42 It is an offence for a person in receipt of a section 27 direction to fail to comply with it (see section 31(3)(a) of the Act). The regulator could also, if it wished to do so, enforce compliance by way of an injunction or equivalent (see section 31(4)).

1.43 There are further direction-making powers in the Act, including power for the Secretary of State to give directions under section 28(3)-(4) and section 29(1).

The full list of guidance documents issued in relation to the Act

1.44 The following guidance documents are available in relation to licences that can be granted under the Act (and any statutory instruments made under the Act):

- Applying for a licence under the Space Industry Act 2018
- Guidance for launch operator and return operator licence applicants and licensees
- Guidance for spaceport licence applicants and licensees
- Guidance for range control licence applicants and licensees
- Guidance for orbital operator licence applicants and licensees
- Guidance for the assessment of environmental effects
- Guidance on security matters for applicants and licensees
- Guidance on the investigation of spaceflight accidents
- Guidance on appealing decisions made under the Space Industry Act 2018 and the Outer Space Act 1986
- Guidance on insurance requirements and liabilities under the Space Industry Act 2018
- Guidance on duties for all licensees under the Space Industry Act 2018 including monitoring and enforcement by the regulator

1.45 In addition, applicants and licensees must follow the Regulator's Licensing Rules and are advised to read the Principles and guidelines for the spaceflight regulator in assessing ALARP and acceptable risk.

Section 2: Legislative Background

The Space Industry Act 2018

2.1 As set out above, the Space Industry Act 2018 regulates all spaceflight activities taking place from the United Kingdom. This includes space activities, sub-orbital activities, and all associated activities.

2.2 Section 23 and Schedule 5 of the Act enable regulations to be developed for the purposes of ensuring security in relation to:

- spaceflight activities
- range control services
- activities associated with spaceflight activities or range control services
- sites and facilities used for or in connection with those activities or services
- spacecraft and their payloads.

The Space Industry Regulations 2021

2.3 Part 3 of the Regulations sets out the prescribed roles which must be in place when applying for a licence and the eligibility criteria which must be satisfied by anyone nominated to undertake a prescribed role. This includes the requirement for the appointment of a security manager for some licence types.

2.4 Part 11 of the Regulations covers security. The Regulations establish the minimum necessary requirements for applicants and licensees to ensure the physical, personnel (regulations 169 – 184) and cyber security (regulations 185 – 186) of space sites, facilities, equipment, spacecraft, carrier aircraft, other vehicles, payloads, cargo, supplies or other things at space sites. Regulations 187 – 190 establish minimum requirements in respect of the training, qualifications and vetting necessary for any persons carrying out security functions associated with spaceflight operations. Furthermore, regulations 192 – 202 address specific requirements for the protection of US technology at a space site.

2.5 Regulation 191 also sets out additional requirements if a space site or operator is declared as Critical National Infrastructure (CNI) or is considered to be providing essential services. Further information is provided below.

Export control legislation

2.6 In addition to the security requirements under the Act outlined in this guidance, the export or transfer of any spacecraft or launch vehicle equipment, software or related technology or other items, is subject to UK Strategic Export Controls, regardless of the origins of those items. Export licence approval is required from the relevant UK authority before any export or transfer of any such items to any destination outside of the customs territory of the UK. As this guidance does not cover UK Strategic Export Controls, the UK's Export Control Joint Unit[4] should be contacted for advice.

Commencement of the Act

2.7 The Space Industry Act 2018 received Royal Assent on 15 March 2020, providing a legislative framework for the licensing of space activities, sub-orbital activities, and associated activities carried out in the UK. However, many of the Act's provisions will only come into force on [date], when the Space Industry

[4] www.gov.uk/government/organisations/export-control-organisation

Regulations come into force. From that date, people and organisations will be able to apply for a licence to:

- launch a launch vehicle from the UK for sub-orbital missions involving human occupants, or return such a launch vehicle to the UK
- launch a launch vehicle from the UK for orbital missions that do not involve human occupants, or return such a launch vehicle to the UK
- procure the launch from the UK of a space object (such as a satellite) into orbit
- operate a satellite from the UK
- operate a spaceport in the UK, or
- provide range control services in the UK

2.8 However, at the point the Regulations come into force, it will not be possible to apply for a licence for some activities that are permitted under the Act. These include:

- the licensing of space activities involving an orbital launch vehicle with human occupants
- the licensing of spaceflight activities involving hypersonic (or any other experimental) transport from A to B

2.9 Such activities are technically complex and difficult to regulate. By their very nature, they will require global collaboration on common standards to a much higher threshold than is achievable with current technologies.

2.10 These restrictions are set out in Commencement Regulations, which also include provisions to ensure that the licensing of a procurement of an overseas launch carried out under the Outer Space Act can continue to be done under that Act, whether such a procurement takes place in the UK or overseas.

Section 3: General security guidance for all licence types

3.1 Security requirements for spaceflight operations should be applied in a manner that is **appropriate** to the activity being undertaken and **proportionate** to the risks entailed. These should be based on a security risk assessment for the space site and operation(s) taking place.

3.2 Appropriate and proportionate levels of security are essential to the success of spaceflight and associated activities in the UK. Security plays a key role in protecting businesses, the people who work for them and the general public. It is also important that the UK meets its international obligations in protecting information and assets used in spaceflight and associated activities. Information and assets used in spaceflight operations may contain sensitive technology. Launch technology, in particular, could be misused for destructive purposes, including the delivery of weapons of mass destruction.[5]

Licence application stage

3.3 At the licence application stage, applicants are required to submit a wide range of information under the Act and under the Regulations and Regulator's Licensing Rules made under that Act. Where applicants are required to have a security manager, they will be asked to submit:

- a draft security programme where applicable, based on a security risk assessment
- a site plan, including proposals for security restricted areas, where applicable
- a cyber security strategy for the proposed operation, and
- where applicable, details of a nominated security manager, responsible for the implementation of security measures

3.4 Applicants should work with the regulator during this stage to address any potential gaps in security. Applicants are also encouraged to engage with the Centre for the Protection of National Infrastructure (CPNI),[6] which can provide advice on protective security risk management. The guidance document Applying for a licence under the Space Industry Act 2018 sets out further information.

3.5 The UK Space Agency (UKSA) is the national authority for National Security risk assessment within the sector. UKSA will work with the regulator to assess applications for National Security implications and make recommendations on issues identified.

3.6 All applicants for a spaceport, range control or launch operator licence are required to appoint a security manager (Part 3, Chapter 1 of the Regulations) who will be responsible for the implementation of the security programme of the spaceflight site or operation. The security manager must be an employee of the applicant or licensee.

3.7 Under regulation 10(2), applicants for an orbital operator licence must have a security manager where the licensed activities may give rise to any issue of national security.[7] For example, an orbital operator's

[5] The UK international obligations and commitments include, for example, UN Security Council Resolution 1540 and the Missile Technology Control Regime (MTCR). Whilst launch vehicle technology can be used for delivery of conventional explosive munitions, the principle area of concern is the delivery of weapons of mass destruction. The MTCR Annex Handbook 2017 provides further information and categorises component parts of rockets and engines.

[6] The Centre for the Protection of National Infrastructure is the government authority for protective security advice to the UK national infrastructure. Its role is to protect national security by helping to reduce the vulnerability of national infrastructure to terrorism and other threats.

[7] "National security" is not defined in either the Act or the Regulations. The regulator, taking advice from government, will determine what it considers to constitute national security, when assessing a licence application.

licence may give rise to issues of national security where sensitive or classified information is involved, or where the operator, the asset being licensed, or the mission management facility are designated as CNI. More information can be found in the Guidance for orbital operator licence applicants and orbital operator licensees.

3.8 Applicants for a return operator licence must appoint a security manager, if the regulator deems that the activities proposed may give rise to any issue of national security. See regulation 9(5) for further clarification.

3.9 Where the regulator identifies a need for a security manager to be appointed on the grounds of national security, this will be set out in licence conditions. Licensees and applicants who are required to have a security manager must adhere to Part 3 of the Regulations. Security managers are required to comply with Part 11 of the Regulations.

Additional security requirements for activities involving US technology

3.10 If an applicant for a launch operator licence wishes to conduct any spaceflight activity involving both US technology and either a non-US launch vehicle or foreign spacecraft, the regulator must be informed of the nationality of any person who has contributed money, equipment, technology or personnel to the production or acquisition of any essential and integral part of the non-US launch vehicle (regulation 202) at the application stage.

3.11 If an applicant for a spaceport licence intends to support launches of US spacecraft or US launch vehicles, the regulator must be informed of the nationality of any person who has contributed money, equipment, technology or personnel to the production or acquisition of any essential and integral part of the launch facilities or its business (regulation 202) at the application stage.

3.12 The requirements under Part 11, Chapter 6 of the regulations are derived from the UK/USA Technology Safeguards Agreement (TSA) (see paragraph 3.25 below).

Space security regulations

3.13 The security requirements relating to spaceflight operations are set out in Part 11 of the Regulations. These are outcome-focused, and the methods licensees employ to comply with Regulations should be appropriate and proportionate to the licensed activity, and all required measures should be implemented as such. Annex A of this document describes key security principles that applicants and licensees are recommended to follow when designing security measures to meet regulatory requirements.

3.14 Section 4 of this document sets out how compliance with the security regulations will be monitored. Non-compliance may result in enforcement action by the regulator.

National Aviation Security Programme

3.15 Not all of the requirements under these Regulations are applicable at horizontal spaceports that are co-located at aerodromes. These aerodromes are required to be directed under the National Aviation Security Programme (NASP), as per regulation 35. The relevant requirements under the NASP will therefore take precedence over the security elements of the Space Industry Regulations, to ensure that the aerodrome remains compliant with the NASP. Details of the publicly available elements of the NASP and further information on how to become a directed aerodrome by the Secretary of State under the Aviation Security Act 1982 can be obtained from the CAA.

3.16 The NASP is comprised of all relevant European Union[8] and domestic legislation detailing aviation security requirements in the United Kingdom. It provides a comprehensive security framework incorporating the EU baseline security requirements retained from EU law, as well as additional "more stringent measures" which are set out in Directions issued by the Secretary of State under Part II of the Aviation Security Act 1982.

Security assessments

Threat assessment

3.17 Security measures should be designed, evaluated and tested according to the level of threat[9] identified in relation to the activity being carried out or the technology being used. Additional security measures, seeking to address emerging threats, may be made by directions by the Secretary of State that are not intended for the general public, as is the case in the aviation sector. Section 28 and section 31 of the Act set out the circumstances in which directions on security may be issued by the Secretary of State.

3.18 The CPNI website (and extranet for registered users) sets out the main threats to national security. All applicants and licensees should be aware of the potential threats associated with their proposed activities and take appropriate precautions.

3.19 Some regulated space sites or satellites in orbit may be designated as CNI,[10] or as essential services[11] in the future. If the Secretary of State, in consultation with the licensee and UKSA, designates a space site or operation as CNI, then the applicant or licensee must:

- take appropriate and proportionate measures to manage any risks posed to the security of the space site and spaceflight activities, and
- cooperate with UKSA (who will consult with CPNI and the National Cyber Security Centre (NCSC)[12]) in ensuring continuity of critical or essential services

3.20 When considering the threats against spaceflight operations, applicants and licensees must give due attention to the potential threat from "insiders". The threat from an insider poses a unique problem given they are likely to have authorised access, enabling them to bypass physical and cyber security measures. Applicants are expected to employ robust security vetting and recruitment practices to mitigate against the insider threat.

[8] The effect of section 3 of the EU Withdrawal Act 2020 is that any EU legislation (including EU Regulation) which was operative immediately before exit day forms part of domestic law after exit day.

[9] Advice on where to find the latest information on the threat to the space sector, and how to carry out a threat assessment, can be provided by the regulator. However, access to such information may be security restricted and applicants/licensees should ensure that a responsible person within the organisation has been security cleared to the necessary level to be provided with such information.

[10] Critical National Infrastructure (CNI) means "those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or, b) significant impact on national security, national defence, or the functioning of the state."

[11] "Essential services" (not currently defined for the space sector outside of these regulations) means services that are essential for the maintenance of critical, societal or economic activities. For example, these include services in the energy sector (electricity, oil and gas); the transport sector (air, rail, water and road); healthcare (hospitals, private clinics and online settings); water (drinking water supply and distribution); and digital infrastructure.

[12] The National Cyber Security Centre (NCSC) acts as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents. NCSC is part of the Government Communications Headquarters (GCHQ).

Security risk assessment

3.21 All organisations who are required to have a security manager must also undertake a security risk assessment of their facilities or activities to determine the level of risk associated with that facility or activity. This assessment must be provided with the draft security programme and other required information at the application stage. The risk assessment will help inform the applicant of the nature and extent of security measures to be put in place through the security programme.

3.22 The extent and detail of assessments undertaken by applicants as part of a security programme, or cyber security strategy, including their independent assessment and verification, should be appropriate and proportionate to the risks identified with the activity taking place. The higher the level of risk, the more comprehensive the security measures should be, leading to greater "defence in depth"[13] protection.

3.23 The regulator can provide guidance on how to undertake Security Risk Assessments, and regulator-approved training courses are also available.[14] The CPNI website (and extranet for registered users) provides information and guidance on Protective Security Risk Management, as well as an Insider Risk Mitigation Framework.

3.24 In carrying out a suitable threat and risk assessment, it is recommended that applicants and licensees take into account a number of factors, including:

- the nature of the operations to be carried out
- regulatory requirements
- overall safety considerations that may be a factor, as a result of security measures
- potential threats
- areas and infrastructure to protect
- risk identification and mitigation

US-based technology systems

3.25 Applicants intending to operate US commercial spaceflight technology from a UK spaceport will need to comply with the US technology specific security regulations specified in Chapter 6 of Part 11, other associated agreements, and US laws and guidance relating to the export (of physical items) or transfer (of software and data/information) of US technology.[15] The definition of "US technology", as set out in regulation 168, is taken directly from the TSA. Any US export licence approval and related Technology Transfer Control Plan (TTCP) relevant to the operation will set out the details of the "US technology" involved.

Byelaws and policing of space sites

Byelaws

3.26 Section 24 of the Act allows for persons authorised to operate a spaceport to make byelaws regulating the use and operation of the spaceport, and the conduct of persons within it, for the purposes of ensuring security in relation to spaceflight operations.

[13] See Annex A of this document.
[14] For more information, contact CAASpaceflightTeam@caa.co.uk
[15] www.trade.gov/us-export-controls

3.27 Before a licensee makes spaceport byelaws that would apply in relation to any part of an aerodrome to which byelaws under section 63 of the Airports Act 1986 apply, the licensee must consult the person who made those byelaws (unless the licensee is that person).

3.28 Schedule 3 to the Airports Act 1986 (further provision about byelaws) applies in relation to spaceports, holders of spaceport licences, and spaceport byelaws, as it applies in relation to airports, airport operators and byelaws under section 63 of that Act.

3.29 Any byelaws made by an authorised person at a space site must be submitted to the Secretary of State for confirmation before coming into force. There is no specific guidance produced by the Department for Transport (DfT) on how to create a byelaw at an aerodrome or space site.

Scotland Freedom to Roam

3.30 Scottish access rights apply to most land and inland water in Scotland. However, licensees of Scottish spaceports will need to take steps to ensure the security of the spaceflight operations from unauthorised access and to protect members of the public from unintentionally accessing a space site, through the implementation of the Space Industry Regulations on security. Further information on freedom to roam is available online.[16]

Policing

3.31 Although there is no requirement to have a police force present at a space site, licensees may wish to consult with local police forces and enter into a police services agreement in relation to the space site. If licensees choose to enter into an agreement with a police force, they must ensure that force is an appropriate compliance authority. This may be confirmed via the regulator.

Physical and personnel security

Security Manager

3.32 All applicants for a spaceport, range control or launch operator licence must appoint a security manager – an employee of the organisation responsible for the implementation of the security programme of the spaceflight site or operation.

3.33 As set out in paragraphs 3.7 and 3.8, applicants for an orbital and return operator licence must have a security manager where the licensed activities may give rise to any issues of national security. For example, an orbital operator's licence may give rise to issues of national security where classified information is involved.

3.34 Regulation 169 sets out the responsibilities of the security manager. These include acting as the focal point for the security programme and managing the development, administration, and maintenance of an effective security operation for the licensee, with responsibility for physical, personnel and cyber security. Training requirements for the security manager are set out in regulation 188.

3.35 The security manager for a horizontal spaceport may be the same person who carries out the security manager functions for an aerodrome co-located with that spaceport.

[16] www.gov.scot/policies/landscape-and-outdoor-access/public-access-to-land/

Security programme

3.36 The security programme must set out the procedures that the applicant or licensee will use to identify any potential security risks and subsequent mitigation measures. Rectification may include having to re-apply security controls to any part of the operation where security may have been breached. The security programme should detail the methods and procedures which the applicant or licensee will follow in order to comply with all applicable regulations.

3.37 The security programme may include drawings, diagrams or maps to assist in understanding the spaceflight operation and any processes that are followed.

3.38 The regulator expects the security programme to be an official company document (i.e. one that includes the company name and logo at the top). The security programme must set out clearly the site or operation to which it relates and the protocols and procedures for maintaining security at that space site or spaceflight operation. There is no mandated format. The programme also needs to include internal quality control provisions describing how compliance with required security measures will be monitored by the applicant or licensee.

3.39 The document should be protectively marked based upon the sensitivity of information it contains once compiled, and only be accessible to those with a need to know. The guidance on Government Security Classifications 2018 may be used as guidelines for protectively marking a security programme.

3.40 It should provide enough detail to give an understanding of the applicant or licensee's businesses and processes for anyone with no knowledge of the spaceflight operation.

Space sites

3.41 Regulation 170 requires the security manager for a space site to draw up and maintain a space site security programme in respect of the site for which they are responsible. In the case of horizontal spaceports, this may be produced as an annex to the existing aerodrome site security programme. The regulation sets out what must be included in the space site security programme, but not the actual content, as this may differ between space sites.

3.42 Once a licence has been granted, the security manager must keep the security programme maintained and up to date in response to any material changes to operations, or incidents that occur that require changes to, for example, procedures. The security manager should review the space site security programme on an annual basis from the date the licence has been granted, to ensure that any changes during the year have been captured, and also ensure that a copy of the most up-to-date version has been provided to the regulator without delay.

Operators

3.43 Regulation 171 requires the security manager for an operator licensee to draw up and maintain a security programme for the spaceflight activities they are responsible for. This applies both to launch operator licensees and to any orbital or return operator licensees that are required to have a security manager. The regulation sets out what must be included in the operator security programme, although the content may differ between operators. Further information as to what is required for orbital operator licence holders, and whether they need a security manager, can be found in the Guidance for orbital operator licence applicants and orbital operator licensees.

3.44 The operator security programme must be integrated with the space site security programme. The intent is to ensure a holistic approach to security across licensed activities.

3.45 Once a licence has been granted, the security manager must keep the operator security programme maintained and up to date in response to any material changes of operations, or incidents that occur that require changes to be made to the programme. The security manager should review the security programme on an annual basis, from the date the licence has been granted, to ensure that any changes during the year have been captured, and then ensure that a copy of the most up-to-date version has been provided to the regulator without delay.

Access control for persons, vehicles, supplies, payloads and launch vehicles

3.46 Regulations 172 – 179 set out requirements for controlling access to space sites for security purposes. Note that some areas may require access control for safety purposes in addition to, or instead of, security; these will be defined by the launch operator's safety case and may be managed by a range control service provider. The security programme should make clear the reasons for which access to an area is controlled. In addition, depending on the nature of the space site and number of spaceflight operations taking place, a security risk assessment should determine the appropriate and proportionate access controls required during active and deactivated periods.

Barriers

3.47 Under regulation 172, licensees must take sufficient security measures to ensure that the space site for which they are responsible is secure from unauthorised access. This may include having a temporary or permanent physical barrier around the site, which is appropriate and proportionate for the site. The CPNI website (and extranet for registered users) provides advice on physical barriers, and further advice may be obtained from the regulator.

3.48 Regulation 172 does not apply to spaceports co-located at NASP directed aerodromes, or other space sites located within the secure perimeter of such aerodrome.

Persons and vehicles

3.49 Regulation 173 sets out the requirements for controlling access to a space site. The regulation describes the conditions to be met before a person or vehicle is allowed to enter a space site. Where there is a requirement to provide details of persons or vehicles in advance, this means the name of the person and their employer, and the make, model and registration number of the vehicle. Licensees should keep a list and examples of appropriate identification at security check points to refer to before access is granted.

3.50 Regulation 173(8) sets out a non-exhaustive list of compliance authorities who can access a space site if they have a legitimate reason for doing so. Persons employed by or on behalf of those authorities will not be granted automatic access rights to space sites because they represent compliance authorities. Instead, they will need to demonstrate that they have a legitimate reason for requesting access to a space site e.g. to carry out a security compliance inspection as part of their duties. They must also meet the access requirements of the space site and provide valid identification as necessary.

3.51 Legitimate reasons include, but are not limited to:

- compliance authority inspections
- the use of security restricted areas as set out in regulation 174
- guided tours
- emergency services responding to a threat to life or property
- individuals carrying out security functions
- vehicles required for specified uses within the space site and security restricted areas or associated with the functions listed above

3.52 As set out in regulation 175, the emergency services must be able to gain access to space sites in the event of an emergency without being subject to normal access control measures. All licensees are required to have an emergency response plan that deals with the safety of their space sites. However, licensees that are required to have security managers and security programmes must also set out a plan for action to be taken following an emergency response at the site, which describes how the licensee will ensure that there have been no breaches in security. This plan must be included in the space site security programme, if the licensee is required to have one.

Prohibited articles

3.53 Regulation 176 sets out requirements around security controls for prohibited articles at space sites. The security controls must be set out in the site security programme, if the licensee is required to have one, and be based on a security risk assessment.

3.54 The list of prohibited articles differs for spaceflight participants and non-spaceflight participants. A spaceflight participant is an individual who is to be carried on board a launch vehicle but is unlikely to be an employee of the launch operator. As such, it is important to ensure that such individuals are not able to carry on to the site and on board the launch vehicle or carrier aircraft any articles that could cause injury or threaten the safety of the vehicle or carrier aircraft.

3.55 All licensees must work together to ensure adequate screening of participants before they enter a security restricted area. Both the regulator and the CPNI website provides advice on the screening of persons and items, as can the DfT Research and Development team.[17] The regulator will look for evidence that the applicant has adequate processes for screening spaceflight participants for prohibited articles.

3.56 Regulation 176 does not apply to a space site located at a NASP directed aerodrome.

Supplies and approval of suppliers

3.57 Regulation 177 sets out the security controls that should be in place to ensure that no prohibited supplies and equipment enter the space site. It does not include payloads or launch vehicles, which are dealt with in regulation 178, but does include anything that is identifiable as supplies and/or equipment to be used, made available, or sold on the space site, or other equipment required to facilitate the activities associated with spaceflight on the ground. The intention is to ensure that prohibited articles are prevented from entering a space site, concealed within such supplies. Supplies could include items such as food, drink, cleaning products, etc. Other equipment could include electronic items. The controls put in place in accordance with regulation 177(1) should be appropriate and proportionate to the supplies entering the site and should be based on a security risk assessment.

3.58 Regulation 179 sets out the procedure for how a licensee must approve a supplier for a space site. For sites with security restricted, controlled or segregated areas, organisations cannot be suppliers unless they have obtained written approval from the licensee. In this regulation, "supplier" means a person who provides items intended to be used, sold or made available for any purpose or activity on the space site. The CAA has published CAP 1260, which is guidance for the approval of airport suppliers. This may be used as a template for spaceport suppliers. However, as there is no mandated format, the licensee should use any form to satisfy itself that the supplier is legitimate. Additionally, both the CPNI and NCSC have produced Supply Chain Security guidance[18], which proposes a series of twelve principles, designed to help

[17] Contact RAD@dft.gov.uk

[18] CPNI: www.cpni.gov.uk/supply-chain; NCSC: www.ncsc.gov.uk/collection/supply-chain-security

an organisation establish effective control and oversight of its supply chain.

Payloads and launch vehicles

3.59 Regulation 178 sets out a number of requirements that licensees must meet before payloads and launch vehicles may enter a space site. It is applicable to all spaceports and launch operators. The regulation is about ensuring the security of the space site prior to the launch of a payload and applies largely to the spaceflight operator.

3.60 Where space site operators are not able, for reasons related to proprietary technology and sensitivity, to screen a payload or launch vehicle, (see paragraphs 3.53 – 3.56) before it enters a security restricted area, spaceflight operators must obtain signed declarations from the providers of those payloads/launch vehicles, in which the providers state they have taken all reasonable steps to ensure the security of the payloads and launch vehicles, from:

- a manufacturer of payloads and launch vehicles
- an operator of payloads and launch vehicles, or
- persons responsible for transporting payloads and launch vehicles from their place of manufacture to the spaceport

Regulation 178 requires one person to be nominated from these three categories, and not one from each. The signed declaration must be obtained before the launch vehicle or payload is transported to the space site. There is no mandated format; however, the declarations should be official company documents. This also includes foreign payloads[19] not licensed under the Act. The Guidance for launch and return operator licence applicants and licensees provides further information on requirements under section 8(2) of the Act.

3.61 The spaceflight operator must provide copies of all relevant declarations to the space site (the security manager) before payloads and launch vehicles can enter security restricted areas. It is recommended that space site security personnel and the launch operator carry out an initial visual inspection on receipt of the payload and launch vehicle.

Space site security restricted and controlled areas

3.62 Regulation 174 sets out the requirements for managing access to all security restricted and controlled areas at space sites.

3.63 Security restricted areas are designated by the Secretary of State.

3.64 Security restricted areas include all areas at space sites designated for:

- assembling, integration and test of spacecraft or carrier aircraft
- mating of spacecraft or carrier aircraft to their payloads
- mission management or range control services (meteorological equipment, tracking systems, surveillance systems, telemetry systems, etc.), where such activities require restricted access
- storage of spacecraft or payloads (at a launch site, launch systems/subsystems may be stored for periods ahead of launch)

[19] "Foreign payloads" refers to payloads that are not covered by an orbital operator licence under the Act, as they are operated from a country other than the UK by a non-UK entity. Launch from the UK still requires a UK launch operator licence, and security checks to determine if the launch raises concerns of national security will include the foreign payload.

3.65 The applicant or licensee who owns/manages the site is required to identify the location and size of all proposed restricted areas. The applicant must provide a site plan that clearly identifies the boundaries of the space site security restricted and controlled areas. This must form part of the licence application process that also includes the submission of the site security programme.

3.66 Controlled areas are space site security restricted areas, that have been designated as such, where US technology, data and equipment is being used, and US launch activity is taking place. The applicant or licensee who owns/manages the site is required to identify the location and size of all proposed controlled areas.

3.67 Regulation 174 sets out specific requirements around access control to both restricted and controlled areas. These include requirements to:

- ensure that these areas are clearly defined and signposted
- ensure that access controls are in place at all times, including for authorised persons to wear identification at all times in such areas
- prevent any prohibited articles (see regulation 176) from entering the area

Surveillance of space sites

3.68 Regulation 180 sets out requirements on licensees around surveillance of the space sites in respect of which they are responsible. It is recommended that licensees work together to determine the best means of surveillance. The frequency and means of undertaking surveillance must be based on a security risk assessment conducted by the site security manager, if the licensee is required to have one. The surveillance to be carried out must be appropriate and proportionate (see paragraph 3.1) to the spaceflight operations being conducted at the site. The CPNI website provides advice on surveillance, and further advice may be obtained from the regulator. The security manager should determine procedures to be followed in the event of a breach of security, which should be set out in the security programme.

3.69 This regulation does not apply to a space site located at a NASP directed aerodrome.

Hazardous materials

3.70 Regulation 181 sets out security control requirements for hazardous materials at space sites. This is separate from the requirements for the safe handling of hazardous materials, which is dealt with in regulations covering spaceport safety at Part 9, Chapter 6, and grant of a spaceport licence at Part 5, Chapter 2 of the Regulations, and the Guidance for spaceport licence applicants and spaceport licensees.

3.71 Regulation 181 applies to the storage of radioactive or other hazardous materials at a spaceport or at locations outside the boundaries of a spaceport, for example if propellants and other hazardous materials are stored at a facility beyond the spaceport's boundaries. Special consideration must be given to any statutory or contractual prohibitions, restrictions or conditions that apply to the materials. Materials must be secured and protected in an appropriate manner as set out in the security programme for the space site, to prevent unauthorised access.

Protection of carrier aircraft, launch vehicles or payloads

3.72 Regulations 182-183 cover the requirements associated with the protection of carrier aircraft, spacecraft or payloads at a spaceport. This includes balloons, as described in Section 1(5) of the Act. The intent is to ensure that all such craft are protected from unauthorised access or interference at a spaceport, while also ensuring compliance with any applicable international obligations of the United Kingdom relating to the security of the carrier aircraft, launch vehicles or payloads.

Pre-integration

3.73 Regulation 182 applies regardless of where the craft is parked or kept at the spaceport. It is the responsibility of the spaceport licensee (working with the operator licensee) to ensure that carrier aircraft, launch vehicles or payloads are protected prior to being integrated with each other.

3.74 Licensees (horizontal spaceport and launch) must also comply with the protection of aircraft security requirements at a NASP directed aerodrome. Further information on those requirements can be obtained from the CAA: however, this will only be provided to authorised persons. Applicants and licensees are encouraged to engage with the CAA on these matters, to ensure that they meet the NASP requirements.

Post-integration

3.75 Protection of carrier aircraft, spacecraft or payloads at a spaceport post-integration is set out in regulation 183. Once payloads have been integrated with launch vehicles and carrier aircraft, the launch operator licensee will be responsible for maintaining security of the craft. The spaceport licensee should continue to work with the launch operator licensee. However, the overall responsibility for protection of integrated craft lies with the launch operator until launch has commenced. If the launch vehicle, such as a carrier aircraft, then returns to the spaceport, security measures for that aircraft revert to the pre-integration stage.

Security controls for flight safety systems

3.76 Regulation 184 sets out security controls for flight safety systems and is applicable to spaceflight operators. A flight safety system is a system that provides a controlled means of ending a flight of a spacecraft, for the purposes of ensuring that the operator's spaceflight activities are carried out safely. A flight safety system might be used, for example, to prevent a launch vehicle from reaching a populated area in the event of vehicle failure by way of a controlled termination of the vehicle. As such, the security of the system is crucial. The operator licensee must ensure that appropriate security controls are applied to flight safety systems, in accordance with regulation 184. This must include secure storage of any explosive material, if required for separation systems or flight termination systems, in accordance with current legislation and Health & Safety Executive guidance.[20]

Cyber security

3.77 While there is no dedicated comprehensive cyber security law in the UK, the Government has approached this issue by seeking to raise awareness and to enhance safeguards against cyber attacks. Organisations should take on full responsibility for managing their own risks in respect of protecting their own sensitive data (proprietary information, financial and commercial data).

3.78 Regulations 185 -186 set out the cyber security requirements in relation to spaceflight activities and licensees.

3.79 Cyber security regulations for spaceflight activities are intended to ensure that a balanced and proportionate approach to cyber risks and threats is taken by licensees to promote good cyber working practices and maintain recognised security standards and controls.

Cyber security strategy

3.80 Regulation 185 requires all licensees to draw up and maintain a cyber security strategy for the cyber

[20] www.hse.gov.uk/explosives/licensing/storage/index.htm

systems used in relation to the spaceflight operations for which it is responsible. This regulation applies to all licence types.

3.81 The cyber security strategy must be based on a cyber security risk assessment and be appropriate and proportionate for the type of systems operated. Once a licence has been granted, the licensee must keep the strategy maintained and up to date in response to any material changes of operations, or incidents that occur that require changes to the cyber security strategy. Licensees should review the cyber strategy on an annual basis, from the date the licence has been granted, to ensure that any changes during the year have been captured, and then ensure that a copy of the most up-to-date version has been provided to the regulator without delay.

3.82 The intent is that the licensee's cyber security risk assessment informs what is appropriate and proportionate for the particular systems in terms of cyber protection. The degree of risk may change, and the systems may undergo upgrades, so it is important that the strategy is reviewed to reflect an up-to-date picture.

3.83 It is recommended that the cyber security strategy follows best practice guidance and advice from the NCSC website[21] (which also contains contact details for organisations if required), with the use of the Cyber Assessment Framework (CAF). The CAF provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible. The CAA has produced guidance for completing the CAF CAP1850 for aviation, which licensees may refer to for assistance.

3.84 Licensees may also choose to examine any other recognised framework, such as the National Institute for Science and Technology (NIST) Framework.[22] This is voluntary guidance based on existing standards, guidelines and practices for organisations to better manage and reduce cyber security risk, and can help build common understanding in international programmes and projects.

3.85 The UKSA has produced a "Cyber Security Toolkit"[23] to assist companies with an interest in the space sector to improve their cyber security and resilience. The NCSC has an online tool called Exercise in a Box, which is intended to help organisations find out how resilient they are to cyber-attacks and practice their response in a safe environment.

3.86 The regulator will issue further spaceflight-specific cyber security guidance to support compliance with the regulations. Licensees are also expected to comply with the UK's international obligations and other relevant legislation, for example regarding the use of spectrum.[24]

Cyber security risk assessment

3.87 Organisations should follow an effective cyber risk assessment methodology when conducting cyber security risk assessments. There are many cyber risk assessment methodologies to choose from when conducting a risk assessment[25], and the NCSC has produced risk management guidance as well.

[21] www.ncsc.gov.uk/

[22] www.nist.gov/cyberframework

[23] www.gov.uk/government/publications/cyber-security-toolkit

[24] Spectrum means the Ofcom-led licensing process for radio waves/bands to regulate how communications satellites broadcast and receive data and what protections and restrictions are in place in relation to different types of data (e.g. TV signals, GPS, Earth Observation, telecoms etc.).

[25] www.cybok.org/media/downloads/Risk_Management__Governance_issue_1.0.pdf

Organisations are responsible for selecting a suitable cyber security risk assessment methodology. The following areas should be considered when conducting cyber security risk assessments:

- threats
- vulnerabilities
- impact (e.g. potential safety impacts)
- likelihood
- mitigations and existing controls

Data protection

3.88 Where personal data related to spaceflight operations, for example flight crew rosters, customer information or employee information, is held on a system, existing legislation, such as the Data Protection Act 2018 and General Data Protection Regulation, will apply.

Duty to report a notifiable (cyber security) incident

3.89 Under regulation 186, licensees are required to report any notifiable incident to the regulator,[26] within 72 hours of it occurring. A notifiable incident is an event which has an adverse effect on the security of the cyber systems used in relation to spaceflight operations or that could have a significant impact on future essential services provided by the licensee. Further information will be made available by the regulator.

3.90 In addition, licensees may choose to report an incident to the NCSC[27] or UKSA.[28] Reporting an incident to the NCSC or UKSA does not fulfil any legal or regulatory incident reporting requirement. The NCSC request that any incident is reported to it so that it can assess risks and trends. Section 4 of the UKSA Cyber Security Toolkit provides further information on suitable reporting channels, depending on the type of incident which has occurred.

Vetting, clearance, training and qualifications

3.91 Regulations 187-190 set out the requirements for all staff with a security function to obtain appropriate security vetting and clearance, and to have undergone suitable training and gained qualifications. This is in addition to the training, qualifications and medical fitness requirements at Part 7 of the Regulations, covering other staff roles for licensed operations.

National security vetting procedures

3.92 Regulation 187 covers vetting requirements for individuals carrying out a security function at a space site or in connection with spaceflight operations. The regulation applies to security personnel associated with all licence types. The licensee is responsible for ensuring that the appropriate vetting is carried out, although the regulator can provide further guidance on this as needed.

3.93 The security manager must have a level of security clearance which would be regarded as appropriate by the UK government for persons performing security functions in space security restricted areas. This must be at least a valid counter-terrorist check (CTC)[29] clearance, or higher clearance as appropriate, as a condition of being engaged, or continuing to be engaged to carry out security functions.

[26] Contact cyber@caa.co.uk
[27] https://report.ncsc.gov.uk/
[28] Contact resilience@ukspaceagency.gov.uk
[29] www.gov.uk/government/publications/hmg-personnel-security-controls

3.94 Any other individual carrying out security functions as part of their employment must undergo a satisfactory background check as a condition of being engaged, or continuing to be engaged, to carry out security functions. The regulator will be able to provide advice on what level of satisfactory background check is appropriate for the security role being undertaken, and this may encompass the different types of security clearance required for individuals carrying out security functions, particularly if they are working within restricted areas.

3.95 Persons who would need to be vetted include:

- the security manager
- any persons carrying out security functions
- employees of/contractors with software and hardware service providers of network information systems used for the implementation and performance of security controls, where direct access to the systems is granted to them
- individuals who have administrator rights for information management systems and critical supplies used by, or made available to, space sites
- anyone else the licensee deems necessary

3.96 This regulation does not apply to a spaceport located at a NASP directed aerodrome, with the caveat of accessing launch technology, as above.

Vetting in regard to US technology

3.97 Any technology that is specified on the UK Strategic Export Control Lists and/or listed by the by the US International Traffic in Arms Regulations (ITAR)[30] or Export Administration Regulations (EAR)[31] lists is deemed "sensitive" and is subject to specific export controls. For US technology, there are also controls on access by non-US nationals to that technology. Anyone wishing to access controlled US technology must obtain export licence approval from the US authorities to do so.

3.98 For anyone who is required to access launch technology, from the US, UK or any other country, the minimum security clearance level recommended is CTC, as this aligns with commitments to the United Nations Security Council Resolution 1540.[32]

Training and qualifications

Appropriate security training and qualifications

3.99 Regulation 188 covers training and qualifications for individuals performing security functions. If a licensee is required to have a security manager, they must also ensure that that individual has the appropriate training and qualifications necessary to carry out this role. In this context, having the appropriate qualifications means that licensees must be able to demonstrate to the regulator that security managers carrying out security functions have had the appropriate training to do so.

3.100 In the absence of security training entities approved by the regulator for spaceflight activities in the UK, the regulator will allow the licensee (authorised persons only) to have access to the aviation security training syllabuses. This will allow licensees to develop a suitable security training framework with the regulator which is relevant to their activities.

[30] www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987
[31] www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear
[32] www.un.org/disarmament/wmd/sc1540/

3.101 Security managers must ensure that any individuals engaged to perform security-related functions also have the appropriate training and qualifications to carry out those functions, which may include, for example, access control, screening of supplies, surveillance, and general security awareness training (GSAT) for all staff. Further details on who can deliver GSAT are available from the regulator. Where licensees do not have a security manager, it is recommended that they provide staff with GSAT from a DfT approved person or organisation.

3.102 The NCSC has produced cyber security training for staff,[33] which licensees may choose to use as part of their GSAT, or as standalone for cyber training. This can be incorporated into a licensee's training programme. The regulator will produce further guidance on appropriate cyber security training and qualifications.

3.103 Licensees are responsible for ensuring that the individuals mentioned in regulation 188(4) receive the appropriate training in order to carry out the functions mentioned in that regulation. The regulator understands that there are, as yet, no officially approved security training entities within the UK for spaceflight operations. Therefore, the regulator will allow the authorised employees of the licensee to have access to the aviation security training syllabuses, so that a suitable framework can be developed. This framework should take the form of a space security training syllabus.

3.104 Details of the appropriate training and qualification necessary for individuals carrying out security functions must be included in the space site security programme and the operator security programme. This, and any amendments to it, must be submitted to the regulator before coming into effect. Any security training course provided to staff by the licensee, or through a third-party provider, should comply with the syllabus.

Training records and qualifications

3.105 Regulation 189 sets out the requirements concerning the recording of training and qualifications of individuals carrying out security functions.

Renewal of security training

3.106 Regulation 190 covers renewal of security training and applies to all licensees who are required to have a security manager. The licensee is required to ensure that the security manager renews its training in accordance with the regulation. The security manager is required to ensure that staff renew their training in accordance with the regulation.

Critical National Infrastructure and Essential Services

3.107 Regulation 191 applies where the Secretary of State (of the Lead Government Department), in consultation with the CPNI, determines that a space site is critical national infrastructure, or spaceflight activities are essential services (see footnote 11). The UKSA has responsibility for the space sector as a whole and takes the lead in determining if a site or service would meet requirements for becoming CNI. Under the Act, the regulator is responsible for ensuring compliance with security regulations.

3.108 Where a CNI or essential service designation applies, the licensee must take appropriate and proportionate measures to manage any risks posed to the security of the space site and spaceflight activities, and cooperate with the UKSA, CPNI and the NCSC in ensuring continuity of critical or essential

[33] www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

services.

3.109 Further information on how to meet CNI requirements can be obtained from the UKSA, and it is recommended that licence applicants and holders follow relevant guidance from CPNI and NCSC.

Security provisions for the protection of US space technology

3.110 Regulations 192-202 apply to all licence types where US technology, equipment or data associated with US launch activity is present. These regulations underpin the requirements that are set out within the TSA, the bilateral treaty between the US and UK governments on technology safeguards associated with US participation in space launches from the UK. The treaty was entered into on 16 June 2020. As such, the regulations and guidance should be read in conjunction with the TSA. While the TSA is only binding on the governments who signed the treaty, the Regulations include provisions which stem directly from the TSA and which must be adhered to by licensees.

3.111 In cases where a US government authorisation is required to enable an activity to take place, the regulator will provide further information to licensees and explain how such authorisations are granted. Authorisation should come from the US Directorate of Defense Trade Controls (DDTC) and will likely be contained in licence conditions attached to the US export licence. The format should be standard for anyone who needs to access an area with US technology in it, or the technology itself, in the course of their employment duties, including UK government authorities carrying out a compliance related role.

3.112 The following regulations specifically require US Government authorisation:

Regulation	**TSA Article**
Reg 192: Segregated areas	Article IV
Reg 193: Control of access to segregated area	Article VI
Reg 194: Control of access to imported US technology	Article III, V
Reg 195: Monitoring and oversight of US technology	Article VI, VIII
Reg 196: Monitoring and oversight of launch activities	Article VI, VII
Reg 197: Restrictions on the use of and access to US technology	Article VI
Reg 198: Restrictions on importing US technology	Article III
Reg 200: Return of US technology if export licence is revoked	Article IV
Reg 201: Processing of US technology after a normal launch	Article VII
Reg 202: Information about nationality of contributors to launch activities, etc	Article III

3.113 As with all other spaceflight operations, the licensee [security manager] should ensure that a security risk assessment is made regarding US launch activity. The regulations which have been derived from the TSA do not set out specific methodologies for protecting US technology: they are primarily about control of access to that technology and data. However, under UK regulations, licensees must ensure that security programmes detail how that technology will be physically protected. In accordance with Export Control Regulations (EAR and ITAR), a Technology Transfer Control Plan (TTCP) is required to prevent unauthorised export or transfer of controlled items, materials, information, or technology. The US Export Compliance Office should assist with this. US companies who are licensed to operate within the UK should use the TSA (Art IV.5) and the UK regulations as a basis to complete a TTCP, with the measures that have been put in place based on a security risk assessment.

Access to information

3.114 The Guidance on duties for all licensees under the Space Industry Act 2018, including monitoring and enforcement, sets out the duties of licensees. This includes the duty of a licensee to provide information

to the regulator, or an inspector appointed to act on behalf of the regulator, as required or in direct response to an information notice issued by the regulator under regulation 228.

3.115 The only type of relevant information an inspector has no right to require a person to produce is that which attracts legal professional privilege. There is no right for anyone to withhold any information on the grounds that it is confidential or sensitive or relates to US technology and is therefore covered by International Traffic in Arms Regulations (ITAR) or export controls. ITAR may place restrictions on a US person but the TSA and associated MoU aim to ensure that US persons can provide information that the regulator and its inspectors will need.

3.116 Under regulation 241, an inspector can request access to premises and vehicles as they deem necessary in relation to their duties. This includes sites that are restricted or segregated on the grounds of US technology being present.

Segregated areas

3.117 Regulation 192-193 sets out requirements around segregated areas. Segregated areas are required when the licensee intends to carry out US launch activities. This is in addition to the requirement for a controlled area at regulation 174. Authorisation to enter a segregated area can only be granted by the US Government. The licensee is responsible for proposing the area to be designated as segregated by the Secretary of State and the US Government. If a segregated area is required, it is up to entities licensed by the US Government to control access to these areas. This does not mean that only US citizens are allowed within the segregated area: the US Government recognises that UK compliance authorities will be required to access segregated areas in order to carry out their duties, and that some non-US employees of the licensee may need to access segregated areas.

3.118 The area remains designated as segregated only if there is US technology in that area. Where there is no US technology present, or US launch activity taking place, a segregated area may be used for other purposes.

3.119 Emergency services are exempt from access control measures for a segregated area, when responding to a threat to life or property.

3.120 In cases where emergency services take some time to get to a site, designated first responders employed by a licensee should be allowed into a segregated area without access control measures. These persons should be designated as first responders when a licensee informs the US Government who would need authorisation to enter a segregated area.

Control of access to imported US technology

3.121 Regulation 194 requires that a person who owns or is in possession of US technology must ensure that access to that technology is controlled by a person authorised to do so by the US Government throughout the transport of the technology, preparations for the launch of US launch vehicles or spacecraft, and the launch of those vehicles.

3.122 It is an offence for the person who owns or is in possession of US technology not to ensure that access to that technology is controlled by a person authorised to do so by the US Government.

Monitoring and oversight of US technology and US technical data and launch activities

3.123 Regulation 195-196 requires that licensees must not prevent individuals authorised by the US Government from accessing US technology and US technical data located at a controlled or segregated area, or during launch activities. In practice, this is likely to require the space site and special launch operator[34] to be provided with a list of persons authorised by the US Government. Such a list is likely to be provided as part of a US export licence condition.

Restriction on the use of and access to US technology

3.124 Regulation 197 covers restrictions on access to and transfer of US technology and technical data. The regulation makes clear that any project related to spaceflight activities that involve US technology or data must not be used for any other purpose without permission from the US Government and sets out which UK authorities may be authorised to have access to US technology and US technical data. US technology will always be under the control of authorised US participants. Licensees should keep a list and examples of appropriate identification at security check points to refer to, before access is granted.

Restrictions on importing US technology

3.125 Regulation 198 sets out that no UK licensee may take possession of imported US technology, or allow any other UK participant to do so, without the permission of the regulator. The regulator may only give permission if the US Government and UK Government have agreed that the UK participant may take possession.

Security training for spaceflight activities involving US technology

3.126 Regulation 199 sets out the requirements around security training for spaceflight activities involving US technology. Details of the training to be received by staff carrying out such activities should be set out in the security programme and form part of the space security training syllabus set out in paragraph 3.98 for spaceflight operations. Due to the highly sensitive nature of such technology, this applies to anyone who may potentially come into contact with US technology or data, and not just those individuals performing security functions.

Return of US technology if export licence is revoked

3.127 Regulation 200 requires a licensee to return any US technology to the United States or other location in accordance with the US export licence or authorisation where the export licence or the authorisation for export or transfer of US technology is revoked by the US Government. This is likely to be managed on a case-by-case basis, with mutually understood principles between the Secretary of State and the US Government.

Processing of US technology after a normal launch

3.128 Regulation 201 describes the procedures for handling US technology after a normal launch. The regulation makes clear that no UK participant can deal with US-related technology in any manner listed in the regulation without authorisation of the US Government.

[34] "Special launch operator" has the meaning given in regulation 168 of the Regulations. A US-based person that holds a licence to launch from the UK will always be defined as a "special launch operator", as per the Security Regulations, to distinguish them as US-based licensees that have also signed a Technical Assistance Agreement with UK entities.

Information about nationality of contributors to US launch activities, etc

3.129 The requirements in regulation 202 are set out in paragraphs 3.10 and 3.11 of this document, and further detailed in the Regulator's Licensing Rules. Any further changes to information held by a licensee must be made known to the regulator as soon as possible.

Section 4: Compliance monitoring and security incident reporting

Compliance monitoring and enforcement

4.1 Under section 3 of the Act, a horizontal spaceport must be located at an aerodrome that is already CAA licensed and directed for the purposes of the NASP. Horizontal spaceports will therefore be subject to both aviation and space industry legislation and enforcement with regards to monitoring and enforcing compliance with the security requirements.

4.2 The following regulations do not apply to horizontal spaceports:

- regulation 172 on access control to space sites
- regulation 176 on security controls for prohibited articles
- regulation 180 on surveillance of space sites
- regulation 187 on national security vetting procedures

4.3 The following regulations require a licensee to comply with any applicable legislation relating to a NASP directed aerodrome:

- regulation 182 on protection of carrier aircraft, launch vehicle or payload: pre-integration
- regulation 183 on protection of carrier aircraft, launch vehicle or payload: post-integration

4.4 These topics are addressed and enforced through the NASP. Horizontal spaceport licensees should adhere to all of the NASP requirements applicable to the directed aerodrome, although the responsibility for the implementation of the NASP remains with the aerodrome and the nominated directed party.

4.5 The directed party for the aerodrome is responsible for providing any licensee that operates within its boundary details of changes and updates to the aviation security regulations. If licensees are found to be deficient in regard to the listed topics above, enforcement action will be taken against the directed party. This means the relationship between the aerodrome directed party and the holder of any licence granted under the Act, carrying out spaceflight activities at that aerodrome, is of key importance.

4.6 The CAA is responsible for enforcing compliance under the NASP, as well as the Space Industry Act 2018 and the Regulations made under it. Where enforcement measures are deemed necessary, the CAA will provide clear direction on who action is being taken against (aerodrome or spaceport licensee) and under which regime action is to be taken.

4.7 Vertical spaceports and all other space sites outside of the boundaries of a horizontal spaceport, where security measures are required, will only be subject to monitoring and enforcement under the Space Industry Regulations.

4.8 Further information on monitoring and enforcement can be obtained from the regulator, and in the document Guidance on duties for all licensees under the Space Industry Act 2018 including monitoring and enforcement by the regulator.

Security incident reporting

4.8 The CAA can provide further guidance on how to report a security incident.

Annex A: Key security principles

A.1 The following paragraphs describe the main security principles that licence applicants and licensees are recommended to follow. The CPNI website (and extranet for registered users) provides further advice on these principles.

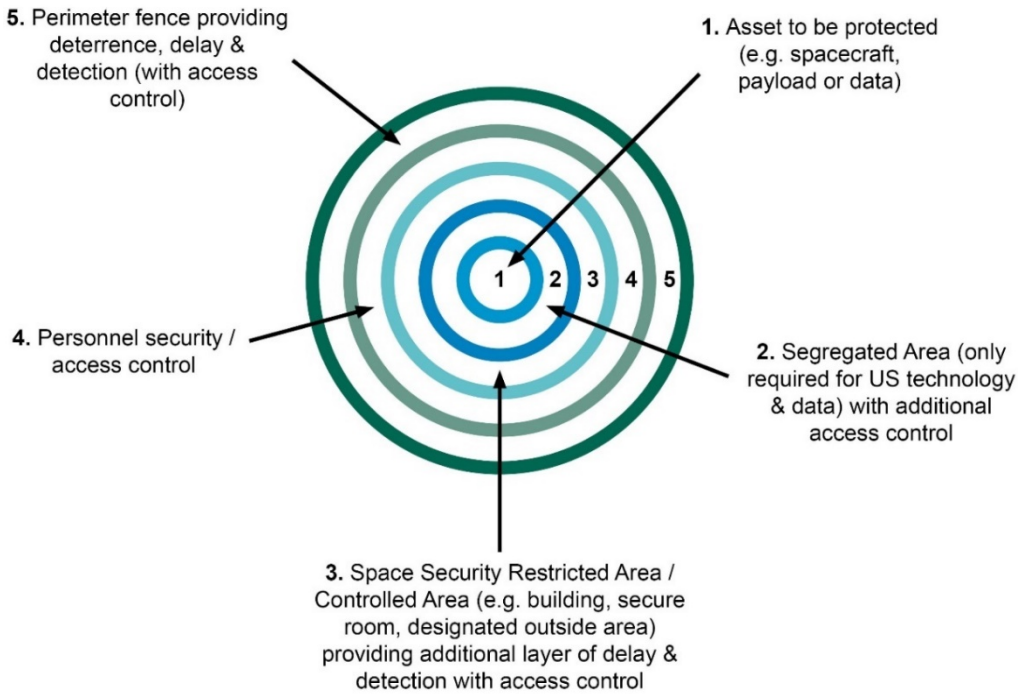
Secure by design

A.2 'Secure by Design' is an approach that seeks to reduce vulnerabilities from the start, rather than attempting to secure or mitigate them post design. It mitigates specific threats by using an approach, design or arrangement tailored to address malicious acts. For example, it is recommended that spaceports, if required by their risk and threat assessment, install measures that prevent unauthorised vehicular access within a requisite distance, to mitigate or reduce the threat of a vehicle-borne improvised explosive device. The installation of such measures may not necessarily be limited to spaceports; secure by design may be applicable at range control service facilities and mission management facilities. Where launch vehicles and payloads are manufactured at facilities not located within a UK spaceport, while not mandated, the regulator recommends a secure design approach be taken. This would be best practice to protect intellectual property from unauthorised access.

Layered security (defence in depth)

A.3 Security measures should reflect a concept of several layers and methods of protection that would have to be overcome or circumvented, to ensure appropriate mitigation of security events if initial prevention fails. Effective physical security of an asset is achieved by multi-layering the different measures: this is commonly referred to as 'defence-in-depth'. The concept is based on the principle that the overall security of an asset is not significantly reduced even if a single layer is breached. Figure 1 illustrates this approach.

Figure 1 – Conceptual model of layered security



Codes and standards

A.4 Space sites and operations that require a greater degree of security (based on their risk and threat assessment), are advised to adopt appropriate and proportionate national or international codes and standards (e.g. British

Standards Institution, International Organisation for Standardisation, Manual Forced Entry Attack Standard) for security structures, systems or components.

A.5 Where there are no established codes or standards relating to space sites/operations, an approach derived from existing codes or standards for similar equipment, in applications with similar security significance, should be adopted. The codes and standards adopted for aviation security would be the most relevant: further information on these may be obtained from the regulator.

A.6 The CPNI also provides a Catalogue of Security Equipment.

Security Management Systems

A.7 Security Management Systems provide a formalised, risk-driven framework for integrating security into the daily operations and culture of a licensee. A Security Management System enables a licensee to identify and address security risks, threats, gaps and weaknesses in a consistent and proactive way. In short, a Security Management System provides the necessary organisational structure, accountabilities, policies and procedures to ensure effective security oversight. Though a Security Management System is not a mandatory requirement to obtain a licence, it is likely to prove helpful to a licensee in ensuring they meet the requirements set out in the Act and related security regulations. A significant proportion of UK airports and UK carriers have adopted a Security Management System and can be a useful source of advice on how to implement a Security Management System. The CAA has issued guidance on how to implement Security Management Systems here.