

Guidance on security matters for applicants and licensees

CAP 2217

Published by the Civil Aviation Authority, 2024

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

You can copy and use this text but please ensure you always use the most up to date version and use it in context so as not to be misleading, and credit the CAA.

First published 2021
Second edition

Enquiries regarding the content of this publication should be addressed to:

commercialspaceflight@caa.co.uk

The latest version of this document is available in electronic format at: www.caa.co.uk

Contents

Chapter 1: Introduction	5
Requirement to obtain a licence	5
Role of the regulator	6
What you need to know	7
Chapter 2: Security requirements when applying for a licence	8
Requirements of all applicants	8
Requirements for applicants who must appoint a security manager	9
Requirements for applicants who propose to import equipment or materials	9
Requirements relating to US technology	9
Exceptions for spaceports hosting horizontal launches	10
Access to security restricted information	10
Granting a licence	10
Duties after you get a licence	11
Legislative background	11
Export control legislation	12
Chapter 3: Complying with space security regulations	13
Security manager	13
Security assessments	14
Threat assessment.....	14
Security risk assessment.....	15
Critical national infrastructure / essential services.....	16
Physical and personnel security requirements	16
Security programme	16
Access controls	19
Surveillance of space sites	24
Hazardous materials	25
Protection of carrier aircraft, launch vehicles or payloads	25
Security controls for flight safety systems.....	26

Chapter 4: Cyber security	27
Cyber security strategy.....	27
Duty to report a notifiable (cyber security) incident.....	28
Chapter 5: Security requirements related to US technology	29
Access to information	29
Segregated areas.....	30
Control of access to imported US technology.....	31
Monitoring and oversight of US technology and US technical data and launch activities	31
Restriction on the use of and access to US technology	31
Security training for spaceflight activities involving US technology.....	32
Other requirements relating to US technology.....	32
Chapter 6: Security duties of licensees	33
National security clearance and vetting procedures	33
Training and qualifications	35
Appropriate security training and qualifications	35
Training for licensees not required to have a security manager	35
Cyber security training.....	35
Training records and qualifications.....	35
Renewal of security training	35

Chapter 1

Introduction

- 1.1 This guidance document summarises the security duties and responsibilities for licensees under the Space Industry Act 2018 (SIA) and the Space Industry Regulations 2021. It tells you about the duties that apply in relation to physical and personnel security to **all** licensees, as well as the specific duties that apply to certain types of licensees. It also explains what you need to do in relation to these security matters when you're applying for a licence.
- 1.2 Security in this document refers broadly to protecting space sites and spaceflight operations from any form of interference that could affect the ability to undertake licensed activities safely and in accordance with UK national security requirements. This includes interference to facilities, equipment, spacecraft, carrier aircraft, other vehicles, payloads, cargo, and supplies at space sites.
- 1.3 Reflecting that, security measures should be applied in a manner that is **appropriate** to the activity being undertaken and **proportionate** to the risks associated with it. Put simply, the launch of a high-altitude balloon from a field would not carry the same security risks as the launch of a rocket, carrying multiple payloads, from a purpose-built spaceport – so fewer security measures would be needed for the balloon launch.
- 1.4 Licensees also have responsibilities in relation to cyber security. These are covered briefly in this document but detailed further in a separate guidance document, [Guidance on Cyber Security Strategies for applicants and licensees \(CAP2535\)](#).
- 1.5 There are additional security requirements for organisations that intend to use US launch vehicles, US related equipment, US technical data or US spacecraft in their operations. In the SIA, Space Industry Regulations and this guidance, these are collectively referred to as “US technology”.

This guidance – like the SIA and Space Industry Regulations – refers to commercial space operations. It does not cover the security of any state sponsored military spaceflight operations from a military launch site.

Requirement to obtain a licence

- 1.6 Under the SIA, if you want to carry out space activities, suborbital activities, and associated activities in the UK, you must get a licence. There are different types of licence covering different activities.

- 1.7 The process for getting a licence is detailed in other guidance documents. It is assumed that readers of this guidance document are familiar with the process set out in [Applying for a licence under the Space Industry Act 2018 \(CAP2209\)](#) and with the specific requirements for the relevant licence type.

Role of the regulator

- 1.8 To get any of these licences, you need to apply to the CAA, we are the UK's spaceflight regulator. We enable space activities which are safe for the public, in line with UK national security and interests and meet the UK's international obligations
- 1.9 We review a range of information about your organisation and the space activities you want to undertake. The information we require is set out in the [Regulator's Licensing Rules \(CAP2221\)](#). We need to understand how you propose to undertake those activities, and what steps you will take to ensure that the risks associated with the activities are as low as reasonably practicable. This includes risks related to security.
- 1.10 In relation to security, we work closely with other relevant authorities, including:
- the UK Space Agency, which is the national authority for national security risk assessment within the sector. The UK Space Agency leads on assessing whether an application for a licence under the SIA, or a proposed application, may have national security implications
 - the National Protective Security Authority (NPSA), which works with partners to identify risks and vulnerabilities to the UK's national infrastructure, and to offer advice to reduce them
 - the National Cyber Security Centre (NCSC)
 - US authorities, including the US Directorate of Defense Trade Controls and US Department of State, in relation to the use of US technology.
- 1.11 We are keen to help applicants understand their security obligations as early as possible. So, we strongly encourage you to contact us before you apply and talk to us about your plans. In this pre-application phase, we can provide a range of support and guidance, including workshops on key aspects of the application.
- 1.12 Once you have applied, we or our partners may need further information about your proposed activities and security measures. We are likely to ask you additional questions about your proposals. We may want to examine documentation, visit sites, see prototype launch vehicles or get demonstrations of technology and systems you propose to use. Our rights to do this are set out in the SIA and Space Industry Regulations. We will treat all information you give us as commercially sensitive.

- 1.13 We will conduct regular monitoring and inspections to check the security measures you have in place. We do have enforcement powers, which we can use if we identify that there are unaddressed security risks, or where we have reasons to be concerned about security.

What you need to know

- 1.14 This document is intended for guidance only. You should read it alongside the [SIA](#), the [Space Industry Regulations](#) and the [Regulator's Licensing Rules \(CAP2221\)](#).
- 1.15 For full definitions of some of the terms used in this guidance, see the SIA and the Space Industry Regulations, in particular [regulation 2](#) and [regulation 168](#). However, there are some definitions elsewhere in the SIA and Regulations.
- 1.16 This guidance focuses on security duties under the SIA and Space Industry Regulations. Depending on what activities you are planning, you may also be required to meet security requirements under other laws and regulatory regimes. During the pre-application phase, we can highlight which other issues may be relevant to your activities, though we can't advise you on how to meet other regulators' requirements.

Chapter 2

Security requirements when applying for a licence

Requirements of all applicants

- 2.1 **All applicants for a licence under the SIA must:**
- provide information about the/your business structure and in particular any foreign ownership or the participation of foreign entities. More details of the specific information required is set out in the [Regulator's Licensing Rules \(CAP2221\)](#).
 - submit a **draft cyber security strategy** for the proposed activities that meets the requirements of [regulation 185](#), plus the cyber security risk assessment on which the strategy is based.
 - complete a **questionnaire**, which explores how your proposed activities will affect UK national security concerns. Questions cover issues such as potential influence from third parties, access to technology and intelligence, reconnaissance, and surveillance issues. Your answers to the questionnaire are reviewed by the UK Space Agency. Depending on your answers and the nature of your proposed activities, the UK Space Agency will work with the National Cyber Security Centre (NCSC), National Protective Security Authority (NPSA) and Ministry of Defence (MOD) as part of the assessment.
- 2.2 This questionnaire helps determine whether your activities might give rise to any issues of national security. Broadly, operations are likely to 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 critical national infrastructure.
- 2.3 If you are applying for an **orbital operator** licence or **return operator** licence, and your proposed activities may give rise to an issue of national security, you must also appoint a security manager. The decision of whether activities may give rise to an issue of national security is made through the UK Space Agency. It will be made as soon as possible during the application process, so you have sufficient time to identify a security manager.
- 2.4 If you are applying for a **launch operator** licence, **spaceport** licence or **range control licence** you must appoint a security manager.

Requirements for applicants who must appoint a security manager

- 2.5 Any applicant who is required to appoint a security manager must submit, as part of your application, details of the individual you propose to appoint, plus:
- a draft **security programme** that addresses the points listed in [regulation 170\(6\)](#) for space sites or [regulation 171\(6\)](#) for spaceflight operators, and
 - the **security risk assessment** on which the programme is based.
- 2.6 The security manager will also be required to undergo relevant UK security vetting.

Requirements for applicants who propose to import equipment or materials

- 2.7 If you intend to bring equipment or material into the UK for use in your space activities, which requires an export licence from the country where the equipment is coming from, you must supply a copy of the **export licence**, or information relating to the progress of an application for an export licence, within your application.

Requirements relating to US technology

- 2.8 If you are intending to use **US commercial spaceflight technology** from a UK spaceport, or support the launches of US spacecraft or launch vehicles from a UK spaceport, you must also comply with the [US technology specific security regulations specified in Chapter 6 of Part 11 of the Space Industry Regulations \(regulations 192-202\)](#). You may also need to comply with associated agreements and US laws and guidance relating to the export (of physical items) or transfer (of software and data/information) of US technology. 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.
- 2.9 If you are applying for a **launch operator** licence and wish to conduct any spaceflight activity involving both US technology and either a non-US launch vehicle or foreign spacecraft, you must inform us 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**.
- 2.10 If you are applying for a **spaceport** licence and intend to support launches of US spacecraft or US launch vehicles, you must inform us 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**.

Exceptions for spaceports hosting horizontal launches

- 2.11 A spaceport for horizontal launches must be located at an aerodrome that is directed under the National Aviation Security Programme (NASP), as per [regulation 35](#).
- 2.12 Because the NASP provides a comprehensive security framework, relevant requirements under the NASP will take precedence over the security elements of the Space Industry Regulations. This means that some of the requirements in the Space Industry Regulations do not apply to spaceports at NASP directed aerodromes.
- 2.13 Reflecting that, for horizontal spaceports, the draft security programme may be produced as an annex to the existing aerodrome site security programme.

Access to security restricted information

- 2.14 It is possible that, during your application (or after you have been granted a licence), you may need access to security restricted information. We have the authority to provide such information to a nominated individual or individuals; however, these individuals may need to hold a certain level of UK security clearance, in accordance with the security classification of the information.
- 2.15 The person nominated as your security manager will need to obtain relevant clearance, but if they have not yet been appointed, you may need to obtain security clearance for a different individual.

Granting a licence

- 2.16 Before granting a licence, we must be satisfied that granting a licence to you:
- will not impair UK national security
 - is consistent with the UK's international obligations, such as those under the [Outer Space Treaty 1967](#), and international commitments, such as those under the [Missile Technology Control Regime](#), and
 - is not contrary to the national interest.
- 2.17 The details you provide in your application should provide us with evidence that you:
- have identified and understood the potential security and cyber security risks to your operations
 - proposed proportionate and appropriate measures to control those risks
 - have the capacity to put those measures into effect, if you are granted a licence.

Duties after you get a licence

2.18 Once you get a licence, you must:

- maintain appropriate and proportionate levels of security at the space site, or in relation to your operations
- provide security training to all those identified as needing it
- obtain relevant national security clearance for those identified as needing it
- put in place the cyber security strategy that was set out in your application (or any elements that weren't already in place)
- appoint a security manager, if you are required to do so
- where you were required to submit a draft security programme, put in place the relevant security measures that were set out in your draft security programme, plus measures to address any additional security requirements we set out as conditions on your licence
- review the security risk assessment on an ongoing basis
- review the cyber security strategy and (where applicable) the security programme at least annually and inform us of certain proposed changes **before** they are implemented
- inform us of any security incidents.

Legislative background

2.19 Security requirements are defined primarily in the Space Industry Regulations 2021, and in particular [part 11](#).

2.20 The regulations in part 11 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 and supplies at space sites.

2.21 [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.

2.22 [Regulation 191](#) 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.

2.23 [Regulations 192 – 202](#) address specific requirements for the protection of US technology at a space site.

Export control legislation

- 2.24 In addition to the security requirements 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, it is recommended you contact the UK's [Export Control Joint Unit](#) for advice.

Chapter 3

Complying with space security regulations

- 3.1 This chapter applies to:
- Launch operator licence applicants/licensees
 - Range control licence applicants/licensees
 - Spaceport licence applicants/licensees
 - Orbital operator licence applicants/licensees, whose activities may give rise to issues of national security
 - Return operator licence applicants/licensees, whose activities may give rise to issues of national security.
- 3.2 The chapter examines each of the security requirements relating to spaceflight, spaceport or range control operations that are set out in [Part 11 of the Space Industry Regulations](#). These are the requirements that you must consider in your draft security programme when applying for a licence, and then address with relevant security measures when you have a licence.
- 3.3 These requirements are intended to be outcome-focused, and the methods you employ to comply with regulations should be appropriate and proportionate to the licensed activity.
- 3.4 Not all requirements are relevant or applicable to all types of operations. It's your responsibility to identify which do apply in your case.

Security manager

- 3.5 [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.
- 3.6 As set out earlier, if you are required to have a security manager, you must provide us with details of the person you propose to appoint when you are applying.
- 3.7 Before the security manager can take up their role, they must hold the level of security clearance which would be regarded as appropriate by the UK

Government for persons performing security functions in space security restricted areas.

- 3.8 The nominated security manager must undergo a background check before you employ them. Currently, the accepted level for this is the [baseline personnel security standard \(BPSS\)](#).
- 3.9 Once they have passed the background check, the security manager should apply for [counter-terrorist check \(CTC\)](#) clearance, or higher clearance as appropriate, as a condition of being engaged, or continuing to be engaged to carry out security functions. Further [guidance on clearance levels](#) is available online.
- 3.10 Once appointed, the security manager must undergo appropriate security training, unless they have existing qualifications. They then in turn are responsible for overseeing the security training, to the appropriate level, of all the other staff.
- 3.11 The security manager is also responsible for conducting security assessments and implementing and monitoring the security programme.
- 3.12 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.

Security assessments

Threat assessment

- 3.13 Security measures should be designed, evaluated and tested according to the level of threat identified in relation to the activities that will be carried out or the technology that will be used.
- 3.14 The NPSA website sets out the [main current threats to national security](#). All applicants and licensees should be aware of the potential threats associated with their proposed activities and take appropriate precautions.
- 3.15 Threat assessment should be considered an ongoing activity. An initial threat assessment will inform your draft security programme; however, the assessment may need to be revisited during the application phase, as well as after you have been granted a licence.
- 3.16 In addition, as in the aviation sector, the Secretary of State can issue directions to implement security measures designed to address emerging threats. Such directions are not intended for the general public. [Section 28](#) and [section 31](#) of the SIA set out the circumstances in which directions on security may be issued by the Secretary of State.

Inside threats

- 3.17 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 some physical and cyber security measures. You should employ robust security vetting and recruitment practices to mitigate against the insider threat.

Security risk assessment

- 3.18 All organisations who are required to have a security manager must 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.
- 3.19 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.
- 3.20 The extent and detail of assessments undertaken by applicants as part of a security programme, 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.
- 3.21 In carrying out a suitable threat and risk assessment, you should take into account, as a minimum:
- 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.
- 3.22 Security risk assessment should be considered an ongoing activity. An initial risk assessment will inform your draft security programme; however, the assessment may need to be revisited during the application phase, as well as after you have been granted a licence, as different risks emerge, or the level of risk changes.

Security risks and the safety case

- 3.23 Because security risks could affect safety of spaceport or spaceflight operations, the security risk assessment must also be considered in the hazard identification

process when developing the safety case for a spaceport, launch operator or return operator licence application.

Information and guidance on [protective security risk management](#) and [insider risk mitigation](#) can be found on the NSPA website.

Critical national infrastructure / essential services

- 3.24 Some regulated space sites or satellites in orbit may be designated as critical national infrastructure (CNI) or as essential services.
- Critical National Infrastructure (CNI) refers to elements of infrastructure whose loss or compromising could result in major detrimental impact on the availability, integrity or delivery of essential services and/or significant impact on national security, national defence, or the functioning of the state.
 - Essential services are services that are essential for the maintenance of critical, societal or economic activities, such as for energy supply, transport, healthcare, water and digital infrastructure.
- 3.25 This designation can happen before a licence is granted, when a licence is granted, or after a licence has been in effect. If the Secretary of State, in consultation with you and the UK Space Agency, designates a space site or operation as CNI, then you 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 UK Space Agency, who will consult with the NPSA and NCSC in ensuring continuity of critical or essential services.

Physical and personnel security requirements

Security programme

- 3.26 The security programme is the basis for meeting the security requirements. It is where you set out the measures you will use, or have used, to:
- identify and understand the potential security risks to your operations
 - control those risks in a proportionate way
 - mitigate any potential breaches.
- 3.27 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.
- 3.28 It should build on the risk assessment and address all relevant regulatory requirements in chapter 11 of the Space Industry Regulations. These are slightly

different for space sites and for operators. They are summarised in the next two paragraphs and examined further later on in this chapter.

- 3.29 For space sites – that is, a spaceport, a mission management facility or a site used in connection with the provision of range control services – the security programme must cover the following requirements, as set out in [regulation 170](#):
- (a) any physical barrier for the space site provided under [regulation 172](#),
 - (b) the access controls to the space site put in place to prevent unauthorised access provided under [regulation 173](#),
 - (c) the space site security restricted areas and controlled areas at the site (see [regulation 174](#)),
 - (d) the access controls for emergency services and post-emergency security procedures provided under [regulation 175](#),
 - (e) security controls relating to prohibited articles (see [regulation 176](#)),
 - (f) the access controls for supplies, payloads and launch vehicles provided under [regulations 177](#) and [178](#),
 - (g) guidance and procedures for assuring and approving suppliers (see [regulation 179](#)),
 - (h) the methods and procedures for surveillance of space sites provided under [regulation 180](#),
 - (i) procedures for protection of hazardous material from unauthorised interference (see [regulation 181](#)),
 - (j) the methods and procedures for protection of carrier aircraft, launch vehicles and payloads at a spaceport pre- and post-integration (see [regulations 182](#) and [183](#)),
 - (k) the training, qualifications and national security vetting procedures necessary for individuals carrying out security functions at the space site provided under [regulations 187](#) to [190](#),
 - (l) the procedures in place for protection of US technology at the site (see [regulations 192](#) to [202](#)),
 - (m) the security measures in place for a space site used in connection with the provision of range control services, and
 - (n) how compliance with methods and procedures specified in the programme is to be monitored by the security manager.

- 3.30 For operators – that is, all launch operators and orbital and return operators that are in scope - the security programme must cover the following requirements, as set out in [regulation 171](#):
- (a) the appropriate measures for protecting launch vehicles, payloads and carrier aircraft at the spaceport (see regulations [182](#) and [183](#)),
 - (b) the appropriate security controls for flight safety systems (see regulation [184](#)),
 - (c) the appropriate training, qualifications and national security vetting procedures necessary for individuals carrying out security functions for the operator (see regulations [187](#) to [190](#)),
 - (d) how compliance with methods and procedures mentioned in this paragraph is to be monitored by the security manager, and
 - (e) the procedures in place for protection of US technology at the site (see regulations [192](#) to [202](#)).
- 3.31 These definitions mean that some operators may need to produce a space site security programme for their mission management facilities. However, 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. All relevant licensees are expected to work together to this effect.
- 3.32 Though there is no mandated format, the security programme should:
- be an official company document (i.e. one that includes the company name and logo at the top)
 - 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 [Government Security Classifications policy](#) may be used as guidelines for protectively marking a security programme.
- 3.33 It can include drawings, diagrams and maps to assist in understanding the spaceflight operation and any processes that are followed. It might also include details of personnel requirements or training, and any responsibilities that might fall to other licensees.
- 3.34 You should also include detailed information about how the methods and procedures you intend to use will be implemented, and how you will monitor compliance with security measures.
- 3.35 These requirements all apply to the draft security programme, which should be as complete as possible, to enable us to assess its suitability.

- 3.36 If any information related to the security programme is provided via separate documents, this should be clearly signposted in the main security programme, setting out exactly where this information is found. When applying for a licence, copies of these other documents must be submitted alongside the security programme.

The link between the draft security programme and the actual one

- 3.37 When you draw up the security programme, it should be based on the draft programme submitted as part of your application. If there are any changes to this, you should let us know, setting out the reasons for the change. You should also reassess the risks based on these changes.

Maintaining the security programme

- 3.38 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 be made to the programme or specific procedures.
- 3.39 As a minimum, 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.
- 3.40 Once the programme has been reviewed, the security manager must provide us with a copy of the most up-to-date version without delay.

Access controls

- 3.41 [Regulations 172 – 179](#) set out requirements for controlling access to space sites, and parts of space sites, for security purposes. Some of these requirements may need to be addressed in operator security programmes.
- 3.42 Access controls should be appropriate and proportionate to the security risk. There may need to be multiple access controls – some for the whole site and some for specific areas. There may also be a need for different levels of access control at different times of the operations. For example, there may need to be increased controls once a launch vehicle, payloads or particular materials are on site.
- 3.43 Some areas of space sites 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.
- 3.44 In your security programme, you should highlight all areas where there are access controls and make clear the reasons for which access to an area is controlled.

Barriers

- 3.45 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.
- 3.46 In your draft security programme, you should indicate the intended location of any barriers and when they would be in operation. Once you get a licence, you are required to put those barriers in place.
- 3.47 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

- 3.48 [Regulation 173](#) sets out the requirements for controlling access to a space site. The regulation makes clear that people and vehicles should only be allowed access to a site if they have a legitimate reason for being there. They must then provide identification, and where appropriate vehicle details, sometimes in advance.
- 3.49 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. However, persons employed by or on behalf of those authorities should 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.
- 3.50 In your draft security programme, you should indicate where and how identification will be checked. Once you get a licence, you are required to implement these procedures.
- 3.51 As set out in [regulation 175](#), access control measures do not apply to the emergency services, when they need to gain access to space sites in the event of an emergency. However, in your security programme, you should 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.

Prohibited articles

- 3.52 [Regulation 176](#) sets out requirements around security controls for prohibited articles at space sites. There are different lists of prohibited articles for employees going about their duties and for spaceflight participants.

- 3.53 There may be different requirements for entry to the site as a whole, entry to any security restricted areas, and boarding a launch vehicle.
- 3.54 Your draft security programme should set out how you will check for prohibited articles. The [guidance on search and screening on the NPSA website](#) may be useful in developing your processes.
- 3.55 Once you get a licence, you are required to put in place the relevant procedures.
- 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. Supplies could include items such as food, drink, cleaning products, etc that are intended to be used, made available, or sold on the space site. Other equipment is anything required to facilitate the activities associated with spaceflight on the ground, such as electronic items.
- 3.58 The intention is to ensure that prohibited articles are prevented from entering a space site, concealed within such supplies.
- 3.59 In your draft security programme, you should describe how you will put in place these controls, in a way that is appropriate and proportionate to the supplies entering the site and that reflects your security risk assessment. Once you get a licence, you are required to put the controls in place.
- 3.60 [Regulation 179](#) sets out the procedure for how a licensee must approve a supplier for a space site. 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.
- 3.61 For sites with security restricted, controlled or segregated areas, organisations cannot be suppliers unless they have obtained written approval from the licensee.
- 3.62 In your draft security programme, you should describe how you will manage this approval process. Once you get a licence, you are required to ensure that you do not use any supplier that is not approved.
- 3.63 The CAA’s [Guidance for Airport Operators Designating Known Suppliers of Airport Supplies \(CAP 1260\)](#) may be a useful template for this. However, as there is no mandated format, the licensee should use any form to satisfy itself that the supplier is legitimate. Additionally, the NPSA’s [supply chain guidance](#) may be useful.

Payloads and launch vehicles

- 3.64 [Regulation 178](#) sets out requirements that licensees must meet before payloads and launch vehicles may enter a space site. It is applicable to all spaceports and launch operators.
- 3.65 Though this regulation is about ensuring the security of the space site prior to the launch of a payload, its implementation will largely be the responsibility of the spaceflight operator.
- 3.66 Under the regulation, all payloads and launch vehicles should be security screened before they enter a security restricted area. Where this is not possible for reasons related to proprietary technology and sensitivity, spaceflight operators must obtain a signed declaration from one of:
- the manufacturer of the payload/launch vehicle
 - the operator of the payload/ launch vehicle,¹ or
 - persons responsible for transporting payloads and launch vehicles from their place of manufacture to the spaceport
- in which the provider states they have taken all reasonable steps to ensure the security of the payloads and launch vehicles.
- 3.67 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.
- 3.68 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.
- 3.69 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.
- 3.70 In your draft security programme, you should summarise how you will meet this requirement. Once you have a licence, you must ensure that you adhere to the process and obtain the relevant declaration(s).

Space site security restricted and controlled areas

- 3.71 [Regulation 174](#) sets out the requirements for managing access to all security restricted and controlled areas at space sites.
- 3.72 Security restricted areas include all areas at space sites designated for:
- assembling, integration and test of spacecraft or carrier aircraft

¹ The operator of a launch vehicle is likely to be the launch operator licensee.

- 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).

- 3.73 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.
- 3.74 Security restricted areas can only be designated by the Secretary of State. In your draft security programme, you must identify the location and size of all proposed restricted areas and provide a site plan that clearly identifies the boundaries of the space site security restricted and controlled areas.
- 3.75 You will need to send a proposal to the Secretary of State for the designation of a space site security restricted area and controlled areas that is based on your draft security programme. Your proposal should explain what activity will be taking place, and where, how it will be access controlled and why it's required, for example segregation of US technology. Proposals should be sent by email to SpaceTeam@dft.gov.uk
- 3.76 Because designation can take some time, you are encouraged to provide this information as soon as possible in the application process – possibly before you submit your full application.
- 3.77 Regulation 174 also 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 from entering the area.
- 3.78 In your draft security programme, you should describe the processes you will use for access control. Once you get a licence, you are required to put those processes in place and prevent unauthorised access to these areas.

Byelaws

- 3.79 Under [section 24](#) of the SIA, spaceport licensees are permitted 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.” In other words, you could introduce byelaws to reinforce access controls.

- 3.80 Any such byelaws must be submitted to the Secretary of State for confirmation before coming into force.
- 3.81 Further, if you are proposing to make spaceport byelaws that would apply in relation to an aerodrome which has already implemented byelaws under [section 63 of the Airport Act 1986](#), you must consult the person who made those byelaws (unless the licensee is that person).

Scotland Freedom to Roam

- 3.82 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.²

Policing

- 3.83 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. You can ask us to confirm this.

Surveillance of space sites

- 3.84 [Regulation 180](#) sets out requirements around surveillance of space sites, to ensure security. This regulation does not apply to a space site located at a NASP directed aerodrome.
- 3.85 Surveillance must be appropriate and proportionate to the spaceflight operations being conducted at the site. The methods you use should reflect the security risk assessment.
- 3.86 It is recommended that licensees work together to determine the best means of surveillance. However, in your draft security programme, you should set out how you would propose to conduct surveillance, indicating where another licensee may be responsible.
- 3.87 In addition, your draft security programme should include the procedures to be followed in the event of a breach of security.
- 3.88 Once you get a licence, you are required to conduct surveillance in the way(s) described in your draft programme, **or** in the ways agreed with other licensees. If your actual surveillance procedures differ from those described in the draft

² www.gov.scot/policies/landscape-and-outdoor-access/public-access-to-land/

security programme, you should let us know and provide us with a description of the processes you will use.

- 3.89 The NPSA provides [guidance on video surveillance, access control and detection](#).

Hazardous materials

- 3.90 [Regulation 181](#) sets out security control requirements for hazardous materials at space sites. This is additional to the requirements for the safe handling of hazardous materials.
- 3.91 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). Materials must be secured and protected in an appropriate manner to prevent unauthorised access.
- 3.92 In your draft security programme, you should describe the ways you would protect these materials and keep them secure. Once you get a licence, you are required to put these measures in place.

Protection of carrier aircraft, launch vehicles or payloads

- 3.93 [Regulations 182-183](#) cover the requirements associated with the protection of carrier aircraft, spacecraft or payloads at a spaceport. The intent is to ensure that all such craft are protected from unauthorised access or interference at a spaceport, while also ensuring compliance with the UK's international obligations relating to the security of the carrier aircraft, launch vehicles or payloads.

Pre-integration

- 3.94 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.
- 3.95 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.

Post-integration

- 3.96 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.

- 3.97 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.
- 3.98 The draft security programme should reflect these different responsibilities.
- Applicants for a spaceport licence should describe how they will:
 - protect the carrier aircraft, launch vehicles or payloads pre-integration
 - manage the handover of responsibility to the launch operator post-integration
 - continue to work with the launch operator post-integration.
 - Applicants for a launch operator licence should describe how they will:
 - protect the carrier aircraft, launch vehicles and payloads post-integration
 - work with the spaceport operator pre-integration
 - manage the handover of responsibility from the spaceport.
- 3.99 Once you get a licence, you are required to put these processes and measures into effect.

Security controls for flight safety systems

- 3.100 [Regulation 184](#) sets out security controls for flight safety systems. It is applicable to spaceflight operators.
- 3.101 Because of the role flight safety systems play, their security is vital. The spaceflight operator licensee must therefore ensure that appropriate security controls are applied to flight safety systems. 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.³
- 3.102 In the draft operator security programme, you should set out how you will protect the flight safety systems. Once you get a licence, you are required to put these processes and measures into effect.

³ www.hse.gov.uk/explosives/licensing/storage/index.htm

Chapter 4

Cyber security

- 4.1 This chapter applies to **all** licence applicants and licensees.
- 4.2 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.
- 4.3 [Regulations 185 -186](#) set out the cyber security requirements in relation to spaceflight activities and licensees.

Cyber security strategy

- 4.4 [Regulation 185](#) requires all licensees to draw up and maintain a cyber security strategy for the cyber systems used in relation to the spaceflight operations for which it is responsible. This regulation applies to all licence types.
- 4.5 The cyber security strategy must be based on a cyber security risk assessment and be appropriate and proportionate for the type of systems operated.
- 4.6 For further details on how to do this, read [Guidance on Cyber Security Strategies for applicants and licensees \(CAP2535\)](#).
- 4.7 Once a licence has been granted, you must keep your cyber security strategy up to date in response to any material changes of operations, or incidents that occur.
- 4.8 As a minimum, you should review the cyber strategy and underlying risk assessment, on an annual basis, from the date the licence has been granted, to ensure that any changes during the year have been captured.
- 4.9 You must inform us after you have conducted the review. If there are any resulting changes, you must inform us of these and provide us with a copy of the most up-to-date version of the strategy.
- 4.10 The intent is that your cyber security risk assessment informs what is appropriate and proportionate in terms of cyber protection for the IT systems you are using. 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.

Cyber risks and the safety case

- 4.11 Because cyber security risks could affect safety of spaceport or spaceflight operations, the cyber risk assessment must also be considered in the hazard

identification process when developing the safety case for a spaceport, launch operator or return operator licence application.

Duty to report a notifiable (cyber security) incident

- 4.12 Under [regulation 186](#), licensees are required to report any notifiable incident to us within 72 hours of it occurring, by emailing cyber@caa.co.uk.
- 4.13 A notifiable incident is any event of a type that has been determined by the regulator and the licensee as having an adverse effect on the security of the network and information systems used in relation to spaceflight operations and that may have a significant impact on future essential services provided by the licensee. These events are agreed between us and the licensee.
- 4.14 In addition, you may choose to report an incident to the NCSC or UKSA. This is not required for any legal or regulatory purposes but can be useful to these authorities in monitoring evolving 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.

Chapter 5

Security requirements related to US technology

- 5.1 This chapter is applicable to any licence applicant or licensee who intends to use US technology, equipment or data in their space activities.
- 5.2 [Regulations 192-202](#) apply to all licence types where US technology, equipment or data associated with US launch activity is present. These regulations stem directly from the [Technology Safeguards Agreement](#) (TSA), the bilateral treaty between the US and UK Governments on technology safeguards associated with US participation in space launches from the UK.
- 5.3 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. If you are using US technology, you must explain in your security programme how that technology will be physically protected.
- 5.4 Certain activities specifically require US Government authorisation. Where either you or we identify that US Government authorisation is required to enable an activity to take place, we will provide further information and explain how such authorisations are granted. Authorisation should come from the US Directorate of Defense Trade Controls (DDTC) and is likely to 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.

Access to information

- 5.5 In accordance with Export Control Regulations (International Traffic in Arms Regulations (ITAR)⁴ or Export Administration Regulations (EAR)⁵), if you are using US technology, you will need to develop a Technology Transfer Control Plan (TTCP) to prevent unauthorised export or transfer of controlled items, materials, information, or technology. The US Department of State should assist with this.
- 5.6 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.

⁴ www.pmdc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987

⁵ www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

- 5.7 As part of our monitoring of spaceflight activities, we can request information about any aspect of your operations, as can inspectors appointed on our behalf. This includes information about US technology. 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 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 we need to carry out our regulatory duties.
- 5.8 Similarly, 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.
- 5.9 Further details on the duties of all licensees in relation to ongoing monitoring can be found in [Working with the regulators as a licensee under The Space Industry Act 2018 \(CAP2214\)](#).

Segregated areas

- 5.10 [Regulations 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, as discussed in paragraph [3.73](#) of this guidance.
- 5.11 Access to segregated areas must be strictly controlled. Authorisation to enter a segregated area can only be granted by the US Government. 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 to carry out their duties, and that some non-US employees of the licensee may need to access segregated areas.
- 5.12 Segregated areas can only be designated by the Secretary of State and US Government. If you are planning to carry out US launch activities, in your draft security programme, you must identify the location and size of all proposed segregated areas and provide a site plan that clearly identifies their boundaries.
- 5.13 Because designation can take some time, you are encouraged to provide this information as soon as possible in the application process – possibly before you submit the full application
- 5.14 If a segregated area is required, it is up to entities licensed by the US Government to control access to these areas.
- 5.15 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.

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

- 5.17 [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.
- 5.18 In your draft security programme, you should set out how you will work with such authorised persons to control access.
- 5.19 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

- 5.20 [Regulations 195-196](#) set out requirements to permit individuals authorised by the US Government to access US technology and US technical data. In practice, this is likely to require the space site and launch operator 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

- 5.21 [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. It also sets out which UK authorities may be authorised to have access to US technology and US technical data.
- 5.22 US technology will always be under the control of authorised US participants. In your draft security programme, you should set out how you will ensure that no unauthorised individuals can access US technology. For example, you could provide a list and examples of appropriate identification at security check points to refer to, before access is granted.

Processing of US technology after a normal launch

- 5.23 [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.

Security training for spaceflight activities involving US technology

- 5.24 [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 your space security training programme.
- 5.25 Due to the highly sensitive nature of such technology, this training should be provided to anyone who may potentially come into contact with US technology or data, and not just those individuals performing security functions.

Other requirements relating to US technology

Restrictions on importing US technology

- 5.26 [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 our permission. We can only give permission if the US Government and UK Government have agreed that the UK participant may take possession.

Return of US technology if export licence is revoked

- 5.27 [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.

Chapter 6

Security duties of licensees

- 6.1 The core security duty of licensees is to ensure appropriate and proportionate levels of security at the space site or around their operations.
- 6.2 For licensees that are required to appoint a security manager and draft a security programme, once you have a licence you must:
- put in effect the security programme and related measures you proposed in draft as part of the licence application
 - review the security risk assessment on an ongoing basis, and adapt the security programme where necessary
 - inform us of any changes to the security programme.
- 6.3 In addition, **all licensees** must:
- ensure all staff have received security training that is appropriate to their role.
 - ensure any individuals carrying out a security function at a space site or in connection with spaceflight operations have met relevant national security vetting requirements.
- 6.4 All licensees also have duties around the reporting of security incidents. We can provide further guidance on how to report a security incident.
- 6.5 If you don't fulfil any of these duties, we can take enforcement action, that could result in you being prevented from providing the licensed services. More details on the action we can take is included in our [Working with the regulator as a licensee under The Space Industry Act 2018 \(CAP2214\)](#) and our [enforcement policy](#).

National security clearance and vetting procedures

- 6.6 [Regulation 187](#) covers national security vetting requirements for individuals carrying out a security function at a space site or in connection with spaceflight operations. These vary depending on the role.
- 6.7 It is your responsibility as a licensee to ensure that the appropriate vetting is carried out. However, you can decide how you will do this.
- 6.8 **Everyone** who you propose to employ in a role which includes a security function must undergo a background check before you employ them. Currently, the accepted level for this is the [baseline personnel security standard \(BPSS\)](#).

6.9 This requirement applies to:

- 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.

6.10 As set out in chapter 3 of this guidance, your 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.

6.11 Once they have passed the background check, the security manager should apply for counter-terrorist check (CTC) clearance, or higher clearance as appropriate, as a condition of being engaged, or continuing to be engaged to carry out security functions.

6.12 If the security manager is not a UK resident, please contact us for further advice and guidance on what is required.

6.13 Further, anyone who is required to access launch technology should also have CTC clearance. Again, if the person requiring CTC clearance is not a UK resident, please contact us for further advice and guidance on what is required.

For more details of UK security vetting processes, including what the checks involve and the need for applicants to obtain sponsorship, visit <https://www.gov.uk/guidance/united-kingdom-security-vetting-applicant#applying-for-or-renewing-security-clearance>

Vetting in regard to US technology

6.14 Any technology that is specified on the UK Strategic Export Control Lists and/or the US ITAR or EAR lists is deemed “sensitive” and is subject to specific export controls. Anyone wishing to access controlled US technology must obtain export licence approval from the US authorities to do so.

6.15 For US technology, there are also controls on access by non-US nationals to that technology.

Training and qualifications

Appropriate security training and qualifications

- 6.16 [Regulation 188](#) covers training and qualifications for individuals performing security functions.
- 6.17 You must ensure that the individual you nominate as security manager has appropriate training and qualifications to carry out the role. There are no specific requirements for this; however, we will expect to see evidence that you have considered what qualifications may be suitable.
- 6.18 The security manager is then responsible for ensuring that any individuals engaged to perform security related functions receive the appropriate training and qualifications to carry out those functions.
- 6.19 This may include, for example, training around access control, screening of supplies, surveillance, and general security awareness training (GSAT) for all staff.
- 6.20 Because there are, as yet, no specific security training programmes relating to spaceflight activities, the security manager can ask us for access to the aviation security training syllabuses. These can then be used as a basis to develop a suitable security training framework.
- 6.21 Details of the training and qualification necessary for individuals carrying out security functions must be included in your draft security programme.

Training for licensees not required to have a security manager

- 6.22 Where licensees do not have a security manager, it is recommended that they provide staff with GSAT from an approved person or organisation. We can provide details of such people/organisations.

Cyber security training

- 6.23 The NCSC offers a range of cyber security training, 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.

Training records and qualifications

- 6.24 You must keep records of the training and qualifications of individuals carrying out security functions for as long as the individual is engaged to carry out those functions.

Renewal of security training

- 6.25 Security training must be renewed at appropriate intervals. [Regulation 190](#) sets out the renewal schedule, for security managers and individuals with security

functions. 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.