STATUTORY INSTRUMENTS

2021 No. 792

The Space Industry Regulations 2021

PART 11

Security

CHAPTER 1

Interpretation

Interpretation

168. In this Part—

"appropriate authorities" has the meaning given in regulation 184(3);

"controlled area" means a space site security restricted area which—

(a) has US technology,

(b) has launch activities taking place in that area,

(c) is designated as a controlled area by the Secretary of State, and

(d) is prescribed as a controlled area under paragraph 1(1)(a) of Schedule 5 to the Act;

"essential services" means services which are essential for the maintenance of critical societal or economic activities;

"foreign spacecraft" has the meaning given in the Technology Safeguards Agreement;

"launch activities" has the meaning given in the Technology Safeguards Agreement;

"NASP directed aerodrome" means an aerodrome which is subject to the direction of the Secretary of State under sections 12, 13, 13A, 14 and 15 of the Aviation Security Act 1982(**1**);

"network and information systems" has the meaning given in regulation 185(3);

"non-US vehicle" has the same meaning as "Foreign Launch Vehicle" has in the Technology Safeguards Agreement;

"notifiable incident" has the meaning given in regulation 186(2);

"security" in connection with network and information systems has the meaning given in regulation 186(2);

"security operative" means an individual who is engaged by the security manager to perform security functions on behalf of a licensee at a space site;

"segregated area" means an area within a space site which is designated as a segregated area jointly by the Secretary of State and the US Government and is prescribed by the Secretary of State as a segregated area under paragraph 1(1)(a) of Schedule 5 to the Act where the licensee permits access only to persons authorised by the US Government to ensure that on an

(**1**) 1982 c. 36.

uninterrupted basis they can monitor, inspect, access and control access to US technology for the purposes of conducting launch activities;

"spaceflight operations" means—

(a) spaceflight activities;

(b) range control services;

(c) activities associated with spaceflight activities and range control services;

(d) activities associated with launch vehicles and their payloads;

"space site security restricted area" means an area within a space site designated by the Secretary of State for the purposes of the assembling and integration of launch vehicles or carrier aircraft(**2**), mating of launch vehicles or carrier aircraft to their payloads, and mission management or range control services where such activities require restricted access;

"special launch operator" means a person who holds a launch operator licence which authorises the launch of a US launch vehicle or of a launch vehicle carrying a US spacecraft;

"supplies" has the meaning given in regulation 177(2);

"supplier" has the meaning given in regulation 179(4);

"Technology Transfer Control Plan" has the meaning given in the Technology Safeguards Agreement;

"unauthorised access or interference" in connection with the security of systems relating to spaceflight operations has the meaning given in regulation 185(3);

"unlawful occurrences" has the meaning given in regulation 185(3);

"UK participants", "US launch vehicles", "US licensees", "US participants", "US related equipment" and "US spacecraft" have the meanings given in the Technology Safeguards Agreement;

"US" means the United States of America;

"US technology" means any US launch vehicles, US related equipment, US technical data or US spacecraft;

"valid" has the meaning given in regulation 173(8).

CHAPTER 2

Physical and personnel security

Responsibilities of a security manager

169. A security manager is responsible for—

(a) setting security policy, standards and targets,

(b) writing security instructions for staff carrying out security functions,

(c) making decisions affecting security operations,

(d) developing and managing security contingency planning,

(e) undertaking a security risk assessment,

(f) ensuring that individuals carrying out security functions have appropriate training and qualifications and have been vetted in accordance with national security vetting procedures to carry out such functions, and

(g) managing security quality control.

(**2**) "carrier aircraft" is defined in section 2(6) of the Space Industry Act 2018.

Space site security programme

170.—(1) Where there is a requirement to appoint a security manager for a space site(**3**) under Chapter 1 of Part 3 (eligibility criteria and prescribed roles for licensees), the security manager must draw up and maintain a security programme in respect of the space site for which that manager is responsible.

(2) The programme may, in the case of horizontal spaceports, be an annex to the existing aerodrome security plan.

(3) The licensee must comply with the requirements of the programme.

(4) The programme must—

(a) comply with the requirements mentioned in paragraph (5), and

(b) describe the methods and procedures mentioned in paragraph (6).

(5) The requirements are that the programme must—

(a) be kept up to date,

(b) be reviewed no more than 12 months after the date on which the licence was granted and, subsequently, at intervals not exceeding 12 months,

(c) be sent to the regulator as soon as possible following a review referred to in sub-paragraph (b),

(d) comply with international obligations of the United Kingdom and be consistent with such obligations,

(e) be site specific and proportionate to the type of activities being carried out on the site, and

(f) be based on a security risk assessment which—

(i) has been carried out by the security manager,

(ii) is reviewed no more than 12 months after the date on which the licence was granted and, subsequently, at intervals not exceeding 12 months, and

(iii) is kept up to date.

(6) The programme must describe—

(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),

(**3**) "space site" is defined in paragraph 5(3) of Schedule 4 to the Space Industry Act 2018. Regulation 2(2) makes provision for references to "space site" to be treated as if they include references to a ship from which a launch vehicle is launched or is to be launched, on which a launch vehicle or carrier aircraft is landed or is to be landing, spaceflight activities are controlled or are to be controlled, range control services are provided or are to be provided or from or on which one or more of these activities are carried out or are to be carried out.

(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.

(7) In this regulation—

"existing aerodrome security plan" means the plan in force in relation to the aerodrome under section 24AE of the Aviation Security Act 1982(**4**);

"post-emergency security procedures" means the checks carried out by the licensee of all the areas that the emergency services have accessed after the emergency services have left the site to ensure that there has been no breach of security as set out in the space site security programme.

Operator security programme

171.—(1) Where there is a requirement to appoint a security manager under Chapter 1 of Part 3, the security manager for a spaceflight operator ("the security manager") must draw up and maintain an operator security programme ("the programme") for spaceflight activities in respect of which that manager is responsible.

(2) The programme must be integrated with the space site security programme.

(3) The spaceflight operator must comply with the requirements of the programme.

(4) The programme must—

(a) comply with the requirements mentioned in paragraph (5), and

(b) describe the methods and procedures mentioned in paragraph (6).

(5) The requirements are that the programme must—

(a) be kept up to date,

(b) be reviewed no more than 12 months after the date on which the licence was granted and, subsequently, at intervals not exceeding 12 months,

(c) be sent to the regulator as soon as possible following a review referred to in sub-paragraph (b),

(d) comply with international obligations of the United Kingdom and be consistent with those obligations,

(e) be specific and proportionate to the spaceflight activities being carried out by the spaceflight operator, and

(f) be based on a security risk assessment which—

(i) has been carried out by the security manager,

(**4**) 1982 c. 36. Part 2A (security planning for aerodromes) of the Aviation Security Act 1982 was inserted by section 79 of the Policing and Crime Act 2009 (c. 26) and applies to NASP directed aerodromes. Section 24AE (aerodrome security plans) was amended by section 15(3) of, and paragraph 186 of Schedule 8 to, the Crime and Courts Act 2013 (c. 22).

(ii) is reviewed no more than 12 months after the date on which the licence was granted and, subsequently, at intervals not exceeding 12 months, and

(iii) is kept up to date.

(6) The programme must describe—

(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).

Access control to space sites: sufficient security measures

172.—(1) A licensee must take sufficient security measures to ensure that the space site for which they are responsible is secure from unauthorised access.

(2) The security measures may include the installation of a temporary or permanent physical barrier around the site.

(3) This regulation does not apply to a spaceport located at a NASP directed aerodrome.

Access control to space sites: further provisions

173.—(1) This regulation applies to the grant of access to a space site.

(2) A licensee may only grant access to a space site if an individual or vehicle seeking to enter the site satisfies the conditions mentioned in paragraphs (3) to (5).

(3) The conditions for granting access to the site are that—

(a) there must be a legitimate reason for the individual or vehicle to be on the site,

(b) the individual seeking access to the site must provide a reliable means of personal identification by providing—

(i) an employee or licensee identification card,

(ii) a national appropriate authority identification card, or

(iii) an approved identification card, and

(c) the individual seeking to bring a vehicle onto the site must provide the licensee with their details, and the details of the vehicle they seek to bring on site, prior to arrival.

(4) In paragraph (3)(a) a legitimate reason for being on the site includes participation in guided tours of the site.

(5) The identification mentioned in paragraph (3)(b) must be checked by an appropriately qualified and authorised security operative to ensure that the identification card is valid and corresponds to the holder before the holder is granted access to the site.

(6) An individual who has been granted access to the site must display any of the personal identification cards mentioned at paragraph (3)(b) at all times whilst on the site.

(7) This regulation does not apply to access for emergency services where they are responding to an emergency on the site.

(8) In this regulation—

"appropriate authority" means a public authority that is responsible for overseeing the operations of the individuals mentioned in the definition of "approved identification card";

"appropriately qualified and authorised security operative" means a security operative who has been trained in accordance with provisions set out in Chapter 4 of this Part and is authorised to carry out security functions on the space site by the licensee;

"approved identification card" means a valid identification card issued by an appropriate authority to the following individuals including—

(a) officers of SAIA,

(b) CAA inspectors and auditors,

(c) a constable,

(d) officers of—

(i) the Health and Safety Executive, or

(ii) the Health and Safety Executive for Northern Ireland, and

(e) inspectors of the Department for Environment, Food and Rural Affairs and its agencies;

"employee identification card" means a valid identification card issued by an individual's employer that clearly identifies an individual and the organisation they work for;

"licensee identification card" means a valid identification card issued by the licensee that clearly identifies an individual and the licensee's company;

"national appropriate authority identification card" means a valid identification card issued by—

(a) the Secretary of State for the purposes of enabling the holder to enter a space site to carry out a security inspection to ensure that security operatives are compliant with security measures set out in this Part and in security guidance made under the Act, or

(b) the US Government to enable access to a space site security restricted area(**5**) which has US technology, data or equipment;

"valid" means current and not tampered with.

Space site security restricted area and controlled area

174.—(1) A licensee must make a proposal to the Secretary of State for an area at a space site to be designated by the Secretary of State—

(a) as a space site security restricted area ("the restricted area"), if the licensee intends to carry out the activities mentioned in paragraph (2) in that area, and

(b) as a controlled area if paragraph (3)(a) or (b) applies.

(2) The area proposed by the licensee must be designated by the Secretary of State as a restricted area for the purposes of—

(a) assembling and integration of launch vehicles or carrier aircraft,

(b) the mating of launch vehicles or carrier aircraft to their payloads, and

(c) mission management or range control services where such activities require restricted access.

(3) The restricted area must be designated as a controlled area by the Secretary of State where—

(a) US technology is being used in that area, and

(**5**) See regulation 168 for the definition of "space site security restricted area".

(b) launch activities are taking place in that area.

(4) The licensee must ensure that—

(a) the restricted area or controlled area is clearly defined and that access to the area is controlled by a security operative or by electronic means as appropriate,

(b) access to the restricted area or controlled area is limited to individuals who have been authorised to be in the area,

(c) individuals seeking access to the restricted area or controlled area have valid identification as a condition of being admitted into the area,

(d) individuals, payloads, launch vehicles, supplies and vehicles entering the restricted area or controlled area are subjected to appropriate levels of screening so that prohibited articles (see regulation 176) do not enter the area, and

(e) individuals who have been granted access to the restricted area or controlled area display their identification at all times whilst in the area.

(5) Where it is not possible to screen a payload or a launch vehicle entering the restricted area or controlled area due to its density or sensitivity, the operator must ensure that it obtains a declaration from the individual seeking to bring the payload or launch vehicle into the area confirming that the payload or launch vehicle has been protected from unauthorised interference or tampering during manufacture and transportation.

(6) This regulation does not apply to access for the emergency services where they are responding to an emergency on the site.

Access control to space sites: emergency services

175.—(1) Where the emergency services are responding to an emergency at a space site the licensee must grant access to the emergency services without requiring them to be subject to the access control measures mentioned in regulations 173 and 174.

(2) The licensee must draw up a plan relating to action to be taken following an emergency response at the site.

Security controls for prohibited articles

176.—(1) A licensee must apply appropriate and proportionate security controls to ensure that no prohibited articles are introduced onto the space site, launch vehicles or carrier aircraft either in vehicles, supplies or on persons.

(2) Individuals other than spaceflight participants must not be permitted to carry onto the site the articles mentioned in paragraph (4).

(3) Spaceflight participants must not be permitted to carry onto the site or on board a launch vehicle or carrier aircraft the articles mentioned in paragraph (5).

(4) The prohibited articles for individuals other than spaceflight participants are—

(a) guns, firearms and any other devices that are capable or appear capable of being used to cause injury by discharging projectiles,

(b) any device designed specifically to stun or immobilise,

(c) any explosives, incendiary substances and devices appearing capable of, or being used—

(i) to cause injury, or

(ii) to pose a threat to the safety of launch vehicles or carrier aircraft, and

(d) any other article capable of being used to cause injury and which is not commonly used on the site.

(5) The prohibited articles for spaceflight participants are—

(a) the articles mentioned in paragraph (4),

(b) any tools capable of being used either to cause injury or to threaten the safety of launch vehicles or carrier aircraft, and

(c) any objects capable of being used to cause injury.

(6) This regulation does not apply to a spaceport located at a NASP directed aerodrome.

(7) Paragraphs (2) and (3) do not apply where—

(a) an individual has been authorised by the licensee to carry prohibited articles onto the site,

(b) the licensee has checked that the individual who is carrying one or more articles specified in paragraph (4) is the individual who has been authorised to do so, and

(c) it is necessary for that individual to carry prohibited articles onto the site in order to undertake tasks that are essential for spaceflight operations or for the performance of duties connected with such operations.

(8) The checking requirement in paragraph (7)(b) is only satisfied if the individual presents the authorisation which—

(a) is either indicated on the identification card that grants access to the space site or in a separate declaration in writing, and

(b) indicates the article or articles that may be carried either as a category or a specific article.

(9) The checks mentioned in paragraph (7)(b) must be performed—

(a) before the individual is allowed to carry the article or articles concerned onto—

(i) the site, and

(ii) on board the launch vehicle or carrier aircraft, and

(b) when the individual is challenged by a security operative performing surveillance patrols on behalf of the licensee.

(10) The articles specified in paragraph (4) may be stored on the site provided they are kept in secure conditions.

(11) The articles specified in paragraph (5) may be stored on the site provided they are not accessible to spaceflight participants.

Security controls for supplies

177.—(1) A licensee must ensure that—

(a) appropriate and proportionate security controls are applied to space site supplies entering a space site,

(b) supplies are protected from unauthorised interference or tampering from the point at which security controls are applied until delivery to the site,

(c) it is familiar with any security controls to be applied to supplies prior to delivery onto the site,

(d) suppliers are informed of the requirements and restrictions to be imposed on supplies prior to entry onto the site,

(e) the licensee retains the final authority to allow supplies to enter the site where the provision of security controls to be applied to supplies prior to delivery onto the site is under the control of third parties,

(f) there are procedures in place to enable supplies entering the site to be inspected and screened, and

(g) staff with access to supplies to which security controls have been applied have been recruited and given security awareness training in accordance with the requirements of the Act and Chapter 4 of this Part.

(2) In this regulation—

"space site supplies" means all items intended to be used, sold or made available for any purpose or activity on the space site, and

"supplies" includes equipment but does not include payloads or launch vehicles and supplies shall be considered as space site supplies from the time that they are identifiable as supplies to be used, sold, or made available for any purpose or activity on the space site.

Security controls for payloads and launch vehicles

178.—(1) A spaceflight operator must—

(a) ensure that security controls are applied to payloads and launch vehicles prior to entry into the space site security restricted area ("the restricted area"),

(b) notify the spaceport licensee of the security controls to be applied to payloads and launch vehicles prior to the entry of payloads and launch vehicles into the restricted area,

(c) obtain a signed declaration from a manufacturer of payloads and launch vehicles and a person responsible for transporting payloads and launch vehicles from their place of manufacture to the spaceport or other place from which the launch is to take place or takes place confirming that all reasonable steps have been taken to ensure the security of payloads and launch vehicles,

(d) retain the final authority to allow any payloads and launch vehicles to enter the restricted area,

(e) inform the individual mentioned in paragraph (3) of the security controls to be imposed on the payloads and launch vehicles, and

(f) ensure that staff with access to payloads and launch vehicles to which security controls have been applied have been recruited and given security training in accordance with the requirements of the Act and Chapter 4 of this Part.

(2) The signed declaration mentioned in paragraph (1)(c) must be provided to the spaceflight operator as a condition of the payloads and launch vehicles being admitted into the restricted area.

(3) The individual to be informed of the security controls imposed on payloads and launch vehicles must be a responsible individual nominated by—

(a) a manufacturer of payloads and launch vehicles,

(b) an operator of payloads and launch vehicles, or

(c) a person responsible for transporting payloads and launch vehicles from their place of manufacture to the spaceport.

Access control to space sites: approval of suppliers

179.—(1) A person wishing to be a supplier to a licensee must apply to the licensee for approval.

(2) An application made under paragraph (1) must identify—

(a) the identity of the intending supplier,

(b) details of the supplies that the intending supplier proposes to provide,

(c) the space site where the supplies are to be delivered,

(d) details of individuals who will need access to the space site to deliver supplies, and

(e) details of the intending supplier's security procedures that describe how supplies are protected from unauthorised interference or tampering.

(3) The licensee must provide the applicant with guidance which sets out how the application is to be assessed.

(4) In this regulation "supplier" means a person who provides any items intended to be used, sold or made available for any purpose or activity on the space site.

Surveillance of space sites

180.—(1) A licensee must carry out ongoing surveillance of the space site in respect of which it is responsible, to ensure security of the site.

(2) The surveillance to be carried out on the site—

(a) must be appropriate and proportionate to the spaceflight operations being conducted on the site,

(b) must not follow a predictable pattern, and

(c) may be carried out by using technical equipment which is capable of recording, detecting or preventing security breaches.

(3) The frequency and means of undertaking surveillance must be based on a security risk assessment conducted by the site security manager or the licensee if the space site does not have a security manager.

(4) The security risk assessment referred to in paragraph (3) must take into account the—

(a) size and layout of the site, including the number and nature of operations,

(b) minimum response times for responding to a security incident, and

(c) possibilities and means of undertaking surveillance.

(5) This regulation does not apply to a spaceport located at a NASP directed aerodrome.

Security controls: hazardous material

181.—(1) This regulation applies to hazardous material at the locations mentioned in paragraph (2).

(2) The locations are—

(a) an area at a spaceport designated as a hazardous material storage facility under regulation 158,

(b) an area at a space site used by the licensee for the storage of any hazardous material,

(c) an area at a spaceport designated for the handling or venting of any hazardous material under regulation 159,

(d) an installation at a spaceport capable of storing or dispensing any hazardous material, and

(e) an area at a spaceport designated for the testing of a launch vehicle under regulation 161 which has the potential to cause a major accident hazard.

(3) A licensee must ensure that, at the locations referred to in paragraph (2)—

(a) it takes into account any statutory or contractual prohibitions, restrictions or conditions which apply to the material,

(b) there are appropriate measures in place to—

(i) detect any unauthorised access to, or unlawful interference with, hazardous material, and

(ii) respond to such unauthorised access to, or unlawful interference with, hazardous material.

(4) In this regulation "installation" has the meaning given in regulation 160(6).

Protection of carrier aircraft, launch vehicle or payload: pre-integration

182.—(1) This regulation applies—

(a) to a carrier aircraft prior to integration with a launch vehicle at a spaceport or other place from which the launch is to take place,

(b) to a payload prior to integration with a launch vehicle at a spaceport or other place from which the launch is to take place, and

(c) to a launch vehicle at a spaceport or other place from which the launch is to take place or takes place,

regardless of where a carrier aircraft or launch vehicle is parked or kept at the spaceport or other place.

(2) A licensee must—

(a) take all practicable measures to ensure that the carrier aircraft, launch vehicle or payload is protected from unauthorised access or interference,

(b) ensure that it complies with international obligations of the United Kingdom relating to security of the carrier aircraft or launch vehicle, and

(c) ensure that it complies with any applicable legislation relating to a NASP directed aerodrome.

Protection of carrier aircraft, launch vehicle or payload: post-integration

183.—(1) This regulation applies to security arrangements which are applicable once a payload has been integrated with a carrier aircraft or launch vehicle at a spaceport or other place from which the launch is to take place or takes place.

(2) A spaceflight operator must ensure that—

(a) the payload, carrier aircraft and the launch vehicle are protected from unauthorised access or interference, and

(b) it complies with any applicable legislation relating to a NASP directed aerodrome.

Security controls for flight safety systems

184.—(1) A spaceflight operator must apply the appropriate security controls to all aspects of a flight safety system, including elements of that system within the launch vehicle.

(2) Security controls are appropriate if they ensure that—

(a) the system is not prevented from functioning as intended due to external interference,

(b) the system is transported and stored securely, and

(c) any actual or attempted theft of, or tampering with, the system is immediately reported to the appropriate authorities.

(3) In this regulation "appropriate authorities" includes the police and the regulator.

CHAPTER 3

Cyber security

Spaceflight cyber security strategy

185.—(1) A licensee must draw up and maintain a cyber security strategy for the network and information systems ("the systems") used in relation to spaceflight operations for which it is responsible.

(2) The strategy must—

(a) be kept up to date,

(b) be reviewed—

(i) no more than 12 months after the date on which the licence was granted and, subsequently, at intervals not exceeding 12 months, and

(ii) upon any upgrades made to the systems,

(c) be sent to the regulator following a review referred to in sub-paragraph (b)(i),

(d) be proportionate and appropriate for the type of systems operated,

(e) comply with international obligations of the United Kingdom and be consistent with such obligations,

(f) be based on a security risk assessment which—

(i) has been carried out by the licensee, and

(ii) is reviewed no more than 12 months after the date on which the licence was granted and, subsequently, at intervals not exceeding 12 months, and upon any upgrades made to the systems,

(g) ensure the security of the systems managed by employees or agents of the licensee,

(h) ensure that the systems are protected from—

(i) unauthorised access or interference,

(ii) other unlawful occurrences, and

(iii) cyber threat, and

(i) ensure that the licensee's suppliers and their supply chain specify in their security protocols how they will achieve the cyber security requirements set out in the strategy.

(3) In this regulation—

"cyber threat" means anything capable of compromising the security of, or causing harm to, information systems and internet connected devices including hardware, software and associated infrastructure, the data on them and the services they provide, primarily by cyber means;

"jamming" means a deliberate blocking or interference with a wireless communication system by transmission of radio signals that disrupt information flow in wireless data networks by decreasing the signal to noise ratio;

"network and information systems" in connection with spaceflight operations means—

(a) an electronic communications network within the meaning of section 32 of the Communications Act 2003(**6**),

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, perform automatic processing of digital data,

(**6**) 2003 c. 21. Section 32(1) was amended by S.I. 2011/1210.

(c) digital data stored, processed, retrieved or transmitted by elements covered under sub-paragraphs (a) or (b) for the purposes of their operation, use, protection and maintenance, or

(d) a flight safety system;

"spoofing" means a technique used to gain unauthorised access to computers whereby an intruder sends messages to a computer indicating that the message is coming from a trusted source;

"unauthorised access or interference" in connection with the security of systems relating to spaceflight operations includes hacking, jamming or spoofing of services or other recognised cyber threats;

"unlawful occurrences" includes theft of data.

Duty to report a notifiable incident to the regulator

186.—(1) A licensee must inform the regulator of any notifiable incident promptly and in any event within 72 hours after it becomes aware that a notifiable incident has occurred.

(2) In this regulation—

"notifiable incident" means any event—

(a) 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

(b) that may have a significant impact on future essential services provided by the licensee;

"security" in connection with the network and information systems means the ability of the network and information systems to resist any action that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or the related services offered by, or accessible via, the systems.

CHAPTER 4

Vetting, clearance, training and qualifications

National security vetting procedures

187.—(1) A licensee must ensure that—

(a) the security manager has a level of security clearance which would be regarded as appropriate by the Government of the United Kingdom for persons performing such security functions,

(b) the individuals mentioned in paragraph (2) have obtained an acceptable criminal record certificate under section 113A(1) of the Police Act 1997, or enhanced criminal record certificate under section 113B(1) of that Act(**7**) in relation to the individuals mentioned in paragraph (2) as a condition of being engaged, or continuing to be engaged, to carry out security functions, and

(c) any other individual carrying out security functions as part of their employment has a satisfactory background check as a condition of being engaged, or continuing to be engaged, to carry out security functions.

(**7**) 1997 c. 50. Sections 113A and 113B were inserted by section 163(2) of the Serious Organised Crime and Police Act 2005 (c. 15), and amended by section 79(1) of the Protection of Vulnerable Groups (Scotland) Act 1997 (asp 14), sections 97(2) and 112(2) of, and paragraph 1 of Schedule 8 to, the Policing and Crime Act 2009 (c. 26), section 80(1) of the Protection of Freedoms Act 2012 (c. 9), section 38(1) of the Justice Act (Northern Ireland) 2015 (c. 9) and by S.I. 2012/3006. There are other amending statutory instruments which are not relevant.

(2) The individuals mentioned in paragraph (1)(b) are—

(a) software and hardware service providers of network and information systems used for the implementation and performance of security controls where direct access to the systems is granted to them, and

(b) individuals who have administrator rights for information management systems and critical supplies used by, or made available to, space sites.

(3) This regulation does not apply to a spaceport located at a NASP directed aerodrome.

Appropriate security training and qualifications

188.—(1) A licensee must ensure that—

(a) any individual employed as a security manager has the appropriate security training and qualifications necessary to carry out the role,

(b) any amendments to details of appropriate security training are sent to the regulator, and

(c) details of the appropriate security training include the types of training that will be required for individuals carrying out security functions at the space site.

(2) The regulator must allow the licensee to have access to the aviation security syllabuses to enable the licensee to develop the appropriate security training.

(3) The security manager must ensure that—

(a) all staff, regardless of the capacity in which they are engaged to work at the space site have appropriate general security awareness training before being granted unescorted access to the site, and

(b) the individuals mentioned in paragraph (4), who are engaged to perform security related functions, have the appropriate security training and qualifications to carry out those functions.

(4) The individuals mentioned in paragraph (3)(b) are—

(a) individuals implementing security controls,

(b) individuals who have roles and responsibilities relating to cyber security,

(c) supervisors of the individuals mentioned in sub-paragraph (a), and

(d) individuals, other than spaceflight participants, requiring unescorted access to security restricted areas on the site.

Training records and qualifications

189.—(1) A licensee must keep the records specified in paragraph (2) for as long as an individual is engaged to carry out security functions at the space site.

(2) The records are those relating to training and qualifications which indicate that an individual has the appropriate training and necessary qualifications for the security related functions that the individual has been engaged to perform.

Renewal of security training

190.—(1) A licensee must ensure that security training for the security manager is renewed periodically in accordance with paragraph (3).

(2) The security manager must ensure that—

(a) security training for individuals engaged to carry out security functions at the space site, and

(b) general security awareness training for all staff, regardless of the capacity in which they are engaged to work at the space site,

is renewed periodically in accordance with paragraphs (4) and (5).

(3) The security manager must renew that manager's training after a period of not more than 36 months beginning on the first day of the calendar month following the month in which they last completed their security training.

(4) An individual engaged to carry out security functions must renew that individual's training after a period of not more than 13 months beginning on the first day of the calendar month following the month in which they last completed their security training.

(5) Each member of staff working at the space site must renew that member of staff's general security awareness training after a period of not more than five years beginning on the first day of the calendar year following the year in which they last completed their security awareness training.

CHAPTER 5

Critical national infrastructure and essential services

Spaceflight activities: critical national infrastructure and essential services

191.—(1) This regulation applies where the Secretary of State, in consultation with the Centre for Protection of National Infrastructure ("the CPNI")(**8**), determines that—

(a) a space site is critical national infrastructure, or

(b) spaceflight activities are essential services.

(2) The licensee must—

(a) take appropriate and proportionate measures to manage any risks posed to the security of the space site and spaceflight activities, and

(b) cooperate with the CPNI and the National Cyber Security Centre in ensuring continuity of essential services.

(3) In this regulation "critical national infrastructure", means those critical elements of infrastructure which include 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) 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, or

(b) a significant impact on national security, national defence, or the functioning of the state.

CHAPTER 6

Security provisions for the protection of US technology

Segregated areas

192.—(1) A licensee who intends to carry out launch activities must make a proposal to the Secretary of State and the US Government for an area to be designated as a segregated area for the purposes mentioned in paragraph (2).

(2) The area proposed by the licensee may be designated by the Secretary of State and the US Government for—

(**8**) The Centre for Protection of National Infrastructure ("the CPNI") is part of the Security Service.

(a) the purposes of ensuring that all US spaceflight activities that are subject to an agreement between the United Kingdom and the US Government are secured to prevent the unauthorised transfer of US technology to third parties, and

(b) as long as there is US technology in that area.

(3) The licensee must ensure that the boundaries of the segregated area are clearly delineated.

(4) If any US launch vehicle, US spacecraft or US related equipment, or debris thereof, is recovered and stored after an accident, the area in which it is stored may be designated by the Secretary of State as a segregated area.

Control of access to segregated area

193.—(1) Subject to paragraph (2), a licensee must ensure that no person may enter a segregated area without—

(a) US Government authorisation, and

(b) being escorted by a person authorised by the US Government unless unescorted access has been authorised by the US Government.

(2) Paragraph (1) does not apply to access for the emergency services where they are responding to an emergency at the space site.

Control of access to imported US technology

194.—(1) A person who owns, or is in possession of, US technology must ensure that access to that US technology is controlled by a person authorised to do so by the US Government throughout—

(a) the transport of US technology;

(b) preparations for the launch of US launch vehicles or US spacecraft;

(c) the launch of US launch vehicles;

(d) the launch of US spacecraft.

(2) A person who contravenes paragraph (1) commits an offence.

(3) It is a defence for a person charged with such an offence to show that that person—

(a) did not know, and had no reason to know, that they were the owner of, or were in possession of, US technology, or

(b) took all reasonable precautions and exercised all due diligence to avoid committing the offence.

(4) A person guilty of an offence under paragraph (2) is liable—

(a) on summary conviction in England and Wales, to a fine;

(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding the statutory maximum;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years, or a fine, or both.

Monitoring and oversight of US technology

195.—(1) A licensee must permit any person whom the US Government has authorised to do so to have access to and monitor any US launch vehicle, US spacecraft or US related equipment, in accordance with that person's authorisation from the US Government.

(2) A licensee must not prevent a US licensee from accessing or monitoring the US technology in respect of which that US licensee has an export or transfer licence or authorisation from the US Government.

Monitoring and oversight of launch activities

196.—(1) A special launch operator must permit the US Government to oversee and monitor its launch activities.

(2) If the launch of a US spacecraft is delayed or cancelled, and the special launch operator who holds a launch licence for that launch intends to remove the US spacecraft from its launch vehicle, the special launch operator must notify—

(a) any US participant whom it considers should be notified, and

(b) the US Government.

(3) If the launch of a US launch vehicle or US spacecraft is cancelled, and the special launch operator for that launch intends to load any US technology that was to be used for the launch onto a vehicle, that special launch operator must—

(a) notify any US participant whom it considers should be notified,

(b) notify the US Government,

(c) only use a vehicle approved by the US Government, and

(d) permit any US participant authorised by the US Government to do so to monitor the loading.

Restrictions on the use of and access to US technology

197.—(1) A licensee using US technology for its licensed activities must ensure that that US technology is not used for any purpose other than that for which a US export licence has been granted, unless the US Government authorises it.

(2) A licensee must ensure that projects related to spaceflight activities that involve the launch of a US launch vehicle or a US spacecraft and items imported for use in these projects are not used for any other purpose without permission from the US Government.

(3) The licensee must ensure that—

(a) no person may transfer US technology to another person at a space site subject to the licensee's control without authorisation from the US Government,

(b) access to US technology used for the licensee's licensed activities is restricted to those persons who have been authorised by the regulator and the US Government, and

(c) persons may only unload sealed US technology used for the licensee's licensed activities and deliver it to a controlled or segregated area if supervised by a person who has been authorised by the US Government.

(4) A special launch operator must ensure that no person may transfer US technology used for that operator's launch activities to another person without authorisation from the US Government.

(5) The persons who may be authorised to have access to US technology include—

(a) SAIA,

(b) the Health and Safety Executive, in the case of US technology in Great Britain, or the Health and Safety Executive for Northern Ireland, in the case of US technology in Northern Ireland,

(c) law enforcement agencies,

(d) the regulator, and

(e) the Secretary of State.

(6) In this regulation, "law enforcement agencies" includes the police.

(7) The licensee must inform the regulator of any information that a US licensee has given it from the US export licence or other authorisation of the US Government to transfer US technology.

(8) The regulator must promptly give the Secretary of State any information it receives under paragraph (7).

Restrictions on importing US technology

198.—(1) A licensee which is a UK participant must not take possession of equipment or technology which originated in the US and was imported into the United Kingdom to support launch activities, and must not allow any other UK participant to do so, unless the regulator gives permission.

(2) If the licensee is in possession of any such equipment or technology, that equipment or technology may only be used to support launch activities if the regulator gives permission.

(3) The regulator may give permission under paragraph (1) or (2) only if the US Government and Her Majesty's Government have agreed that the UK participant may have possession of the equipment or technology.

(4) The licensee must comply with any Technology Transfer Control Plan that it has entered into.

Security training for spaceflight activities involving US technology

199. A special launch operator must ensure that all staff carrying out spaceflight activities involving US technology, regardless of whether or not they are carrying out a security function, receive training on security measures required for US technology.

Return of US technology if export licence etc. is revoked

200. A licensee which uses US technology for its licensed activities must ensure that in the event that a US export licence or authorisation for export or transfer of any of that US technology is revoked by the US Government, anything imported under the revoked licence or authorisation is either—

(a) returned to the US in accordance with the US export licence or authorisation, or

(b) sent to another location, if authorised by the US Government.

Processing of US technology after a normal launch

201.—(1) Following the launch of a US launch vehicle or US spacecraft which proceeded as expected, the special launch operator must—

(a) not permit any UK participant to dismantle US related equipment unless that UK participant is authorised to do so by the US Government;

(b) either—

(i) destroy any US related equipment it used for the launch and which it does not need for further launch activities, or

(ii) send such equipment from the UK to a location approved by, and in a manner approved by, the Secretary of State and the US Government;

(c) return any US technical data it has to a location approved by the Secretary of State and the US Government;

(d) not permit any UK participant to take part in the recovery of a reusable US launch vehicle or US related equipment unless that UK participant is authorised to do so by the US Government and is supervised by a US participant;

(e) send any recovered US launch vehicle, recovered US spacecraft, or recovered components of a US launch vehicle or US spacecraft, from the UK to a location approved by, and in a manner approved by, the Secretary of State and the US Government;

(f) not permit any UK participant to study or photograph recovered US technology unless that UK participant is authorised to do so by the US Government.

(2) Where recovery of a reusable US launch vehicle is planned to take place in a country outside the UK, the special launch operator must notify the regulator of the location of the planned recovery at the earliest opportunity.

(3) On receipt of information under paragraph (2), the regulator must inform the Secretary of State promptly.

Information about nationality of contributors to launch activities etc.

202.—(1) An applicant for a launch operator licence that would authorise a spaceflight activity involving both US technology and either a non-US vehicle or a foreign spacecraft must, when it applies for the licence, inform the regulator 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—

(a) the non-US vehicle,

(b) the foreign spacecraft, or

(c) the applicant's launch business.

(2) An applicant for a spaceport licence, if the applicant intends that there will be launches of US spacecraft or US launch vehicles from the spaceport, must, when it applies for the licence, inform the regulator 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 launch business.

(3) The holder of a licence of a kind mentioned in paragraph (1) or (2) must inform the regulator as soon as possible of any change to information provided under paragraph (1) or (2), including any contributions to any new essential and integral part.