
DRAFT STATUTORY INSTRUMENTS

2021 No.

The Space Industry Regulations 2021

PART 11

Security

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⁽¹⁾,
- (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,
- (c) digital data stored, processed, retrieved or transmitted by elements covered under subparagraphs (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.

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