Department for Transport

OFFICIAL

Implementation of the NIS Directive DfT Guidance version 1.1

Moving Britain Ahead

December 2018

The Department for Transport has actively considered the needs of blind and partially sighted people in accessing this document. If you have other needs in this regard please contact the Department.

Department for Transport
Great Minster House
33 Horseferry Road
London SW1P 4DR
Telephone 0300 330 3000
Website www.gov.uk/dft
General enquiries https://forms.dft.gov.uk

Contents

1. Introduction

Purpose and audience

1.1 The purpose of this guidance is to provide an overview of the implementation of the Network and Information Systems Directive (the NIS Directive) in the transport sector, following the coming into force of the UK implementing legislation (the NIS Regulations) on 10th May 2018.

1.2 This guidance is aimed at those organisations that are designated as Operators of Essential Services (OES) under the NIS Regulations within the transport sector in the UK.

1.3 This guidance details the responsibilities of OES as well as the roles and responsibilities of the Competent Authority (i.e. the body responsible for oversight and enforcement of the NIS Regulations within a sector) and how these will be carried out, with particular focus on the first year post-May 2018. It also sets out the process and thresholds for mandatory incident notifications. Further to this, it contains specific guidance for each transport mode and provides clarity on how the NIS Regulations will align with any existing guidance, standards or regulations related to network and information system security.

1.4 This version of the guidance has been issued to assist transport OES with compliance with the NIS Regulations. It has been revised following feedback from industry.

1.5 This guidance will be amended as required to ensure that it remains accurate and up to date. Additional guidance may be added to this document if necessary.

2. Background to the NIS Directive

What is the NIS Directive?

2.1 The NIS Directive is designed to boost the overall level of security for network and information systems that support the delivery of essential services within the EU. It applies to those sectors which are vital for our economy and society, providing services such as the supply of electricity and water and the provision of healthcare and transport.

2.2 This NIS Directive was adopted by the European Parliament in July 2016 and came into force in August 2016, giving Member States 21 months to transpose the Directive into their national laws.

2.3 The aims of the measures set out in the Directive are to improve the security of network and information systems across the EU by:

- Ensuring that Member States have in place a national framework to support and promote the security of network and information systems, consisting of a National Cyber Security Strategy, a Computer Security Incident Response Team (CSIRT), a national Single Point of Contact (SPOC) for other Member States and a NIS Competent Authority (or Authorities);
- Setting up a Cooperation Group and a CSIRT Network; the former to facilitate strategic cooperation and the exchange of information among Member States and the latter to promote swift and effective operational cooperation on incidents and sharing of information about risks;
- Ensuring that organisations within those vital sectors of our economy are effectively managing the security of their network and information systems. Organisations within those sectors that are identified by Member States as “Operators of Essential Services (OES)” will have to:
  - take appropriate and proportionate technical and organisational measures to manage the security of their network and information systems (including managing cyber security risks and broader security and resilience risks to network and information systems);
  - take appropriate measures to prevent and minimise the impact of incidents affecting the security of their network and information systems; and
  - notify the relevant authority of any incidents affecting network and information systems which have a significant impact on the continuity of the essential service they provide.

2.4 In the UK, the NIS Directive applies to the following sectors: energy, health, water, transport and digital infrastructure. Some sectors are exempt where there are provisions within their existing legislation which are, or will be, at least equivalent to those the NIS Directive specifies (e.g. finance and civil nuclear sectors).

UK implementation

Public consultation

2.5 The Government set out its initial proposals for implementing the NIS Directive in a public consultation that ran from 8th August to 30th September 2017. The consultation document included the Government's proposals and asked a series of questions on a range of detailed policy issues relating to transposition. In total the Government received over 350 responses across all sectors with 38 of those coming from the transport sector.

2.6 The responses to the consultation indicated, in general, that there was broad support for the proposals which were viewed as appropriate and proportionate. However, there were some core areas of concern highlighted which required further clarity or changes to the approach. These included areas such as penalties, incident notifications, expectations in the first year and the roles and responsibilities of the Competent Authorities, SPOC and CSIRT.

2.7 The Department for Digital, Culture, Media and Sport (DCMS) published the Government's response to the consultation on 28th January 2018 which sets out the overall policy for UK implementation and addresses concerns raised in the consultation. A link to this document can be found in Annex A.

National Cyber Security Centre

2.8 The National Cyber Security Centre (NCSC) has several critical roles to play in support of NIS Directive implementation. It will be the CSIRT, the national SPOC and the national technical authority.

2.9 As the CSIRT, the NCSC will be responsible for incident response, including monitoring incidents, providing dynamic incident analysis and situational awareness as well as providing early warning alerts and announcements. These are not new functions for the NCSC as it already undertakes these roles at a national level for cyber security incidents.

2.10 As the SPOC, the NCSC will act as liaison on NIS Directive matters with the EU and between different national Competent Authorities. The role includes preparing a summary report of incident notifications and liaising with relevant authorities in other Member States on cross-border incidents.

2.11 As the national technical authority, the NCSC will be responsible for supporting both OES and the Competent Authorities by setting security principles, publishing guidance, developing assessment tools and acting as a source of technical expertise on cyber security.

2.12 All of these roles are advisory; the NCSC will not have any regulatory responsibilities. It will not be able to, or seek to, enforce any actions on an OES. Enforcement will solely be the responsibility of the Competent Authorities.

2.13 As the national technical authority, the NCSC is responsible for two core products which support UK implementation of the NIS Directive. These are:

- **The NIS Security Principles and Guidance Collection**

This comprises a set of outcome-based security principles which form part of the core requirements placed on OES to manage the security of their network and information systems. These are underpinned by a suite of additional guidance which provides further information on how an OES may achieve the outcomes specified in the

principles. The NCSC published their guidance in parallel to the response to the consultation on 28th January 2018. See section 4 of this document for further detail.

- **The Cyber Assessment Framework (CAF)**

This is a tool that provides a systematic method for assessing the extent to which OES are achieving the outcomes specified by the NIS principles. It can be used by Competent Authorities when assessing OES or by OES themselves as a self-assessment tool. The CAF provides Indicators of Good Practice against each element of the security principles in order to be able to assess the maturity of an OES against that particular element. The CAF is available on the NCSC website (a link can be found in Annex A). Note that OES in aviation will be assessed against the cyber security controls framework published by the CAA as CAP 1574 (see section 6 for further details).

3. Implementation in the transport sector

Who is in scope?

3.1 The NIS Directive specifies the types of entities that all Member States should consider for inclusion (Annex II of the Directive). In the UK, designation of organisations as OES has been achieved through setting definitions and thresholds in legislation relating to the scale of an organisation's operations. The thresholds have been defined based on the level of societal or economic impact which could result from disruption to the services those entities provide. Organisations that meet those definitions and thresholds are automatically designated as OES. The definitions and thresholds for designating OES are contained in the NIS Regulations (see Annex A for a link to the full text) and have also been included within the tables in Annex D of this document (which also contains references to the relevant statistics sources).

3.2 In summary, the types of organisations in scope within the transport sector are:

- Owners or managers of airports;
- Air navigation service providers;
- Air carriers;
- Harbour authorities;
- Shipping companies;
- Operators of port facilities;
- Operators of vessel traffic services;
- Operators of railway assets (trains, networks, stations and light maintenance depots) for domestic and international rail plus some light rail and underground services;
- Roads authorities and operators of intelligent transport systems.

3.3 Specific thresholds apply to many of the above types of entities which are generally based on the scale of the operation in terms of annual passenger numbers or freight tonnage. For domestic and international rail there are no specific thresholds and so any entity that meets the definitions will be in scope.

3.4 The NIS Regulations also provide Competent Authorities with the power to designate organisations in scope that do not meet these thresholds but are still considered to provide essential services. This will be used to designate some organisations within the transport sector. Note that Competent Authorities are obliged to review the use of this designation power at regular intervals and the NIS Regulations also set out a process for OES to appeal such designations and request independent review.

Competent Authorities

3.5 Oversight and enforcement of the NIS Regulations is the responsibility of the designated Competent Authority.

3.6 The UK Government decided that a multiple Competent Authority approach, with each Competent Authority having a detailed understanding of the individual sector and their associated challenges, is most appropriate for the UK. Competent Authorities have therefore been designated for each sector or region covered by the NIS Regulations.

3.7 Competent Authorities have the sole authority and responsibility for all regulatory decisions in relation to the NIS Regulations. Competent Authorities will be supported by the NCSC as detailed in section 2 of this document.

Transport Sector Competent Authority

3.8 The Competent Authority for each transport sub-sector is set out in Table 1 below:

3.9

Sub-Sector	Competent Authority
Aviation	Secretary of State for Transport and the Civil Aviation Authority (UK)
Maritime	Secretary of State for Transport (UK)
Rail	Secretary of State for Transport (England, Scotland and Wales) The Department of Finance (Northern Ireland)
Roads	Secretary of State for Transport (England and Wales) The Scottish Ministers (Scotland) The Department of Finance (Northern Ireland)

Table 1 Competent Authorities within the transport sector

3.10 Where the Secretary of State for Transport is the Competent Authority, the Cyber Compliance Team (CCT) in DfT will be responsible for carrying out the roles and responsibilities of the Competent Authority on behalf of the Secretary of State for Transport.

Responsibilities of the Competent Authority

3.11 Competent Authorities are responsible for:

- reviewing the application of the NIS Regulations in their sector or region (see section 5);
- establishing the identification thresholds for the OES in their sector or region (see section 3);
- preparing and publishing guidance to assist OES or Digital Service Providers in meeting the requirements of the NIS Regulations (including this guidance document);
- keeping a list of all OES who are designated and all revocations;

- assessing compliance of OES against the requirements of the NIS Regulations, including audits (see section 5);
- determining the thresholds for notifiable incidents in their sectors or regions (see section 4);
- receiving incident notifications (see section 4);
- cooperating with other Competent Authorities to provide consistent advice and oversight to OES or Digital Service Providers (see section 5);
- consulting and cooperating with the CSIRT, SPOC and Information Commissioner's Office (ICO);
- making sure that there are processes in place for responding to physical security incidents, system failures or natural hazards affecting network and information systems - and issuing guidance to support companies dealing with those types of incidents (see section 4);
- investigating incidents (see section 5);
- enforcement, including issuing notices and penalties, of the requirements of the NIS Regulations (see section 5).

3.12 For the aviation sector, the roles and responsibilities of the Competent Authority will be divided between the Secretary of State for Transport and the Civil Aviation Authority. Further detailed guidance on this can be found within section 6.

4. Requirements on Operators of Essential Services (OES)

Security requirements

4.1 The approach taken to setting the security requirements for OES is one based on principles that are supported by guidance. The NCSC has defined a set of cyber security principles consisting of 14 top-level outcomes, with supporting narratives, which are grouped into four top-level objectives (see Annex B). These principles should be relevant to all network and information systems supporting the delivery of essential services, where is it assessed the compromise of such a system could result in an impact on the continuity of the essential service. The principles carry no assumptions about how the specified outcomes should be achieved. It is for the OES to determine, in discussion with the Competent Authority, the most appropriate security measures to deliver these outcomes within their organisational context. The Competent Authority will need to agree that the measures determined by the OES are appropriate and proportionate for each organisation. The Competent Authority may, in some cases, provide additional guidance to OES on how they can be achieved.

4.2 It is the Government's view that the principles-based approach is a more effective way of driving improvements to cyber security in the context of the NIS Directive than an approach based on prescriptive rules. This is due to the fact that in complex and rapidly changing areas such as cyber security, prescriptive rules can lead to unintended consequences, misallocation of resource and limited benefit. Organisations understand their own business better than any external entity and should be capable of taking informed, balanced decisions about how they achieve the outcomes specified by the principles.

4.3 To support OES in meeting the security principles the NCSC has also published a collection of guidance. Each of the principles is linked to specific guidance which highlights some of the factors that an organisation will usually need to take into account when deciding how to achieve the outcome and recommends some ways to tackle common cyber security challenges.

4.4 Annex A contains a link to the principles and guidance, which includes the NCSC's instructions on how these should be used by OES.

4.5 The NCSC's principles and guidance are primarily focused on ensuring adequate cyber security risk management. However, OES will also need to take into account broader resilience risks when considering the security of their network and information systems. This includes ensuring they are resilient to wider risks such as loss of power supply, hardware or software failure, physical damage and environmental hazards.

4.6 As with cyber risks, it is the responsibility of OES to identify these broader resilience risks to their network and information systems and have appropriate organisational

structures, policies and processes in place to understand, assess and systematically manage them. They should be included in any risk management plan which demonstrates those risks have been assessed and understood, and mitigation measures put in place where appropriate. It is, again, the responsibility of OES to decide what security measures are appropriate within the context of their organisations and in discussion with the Competent Authority.

4.7 Guidance on these risks can be found within the NCSC principles and guidance, for example physical access control within B.2, or system failure and physical resilience within B.5. Other sources of information, such as some common international standards, frameworks and guidance, which could be helpful to OES in addressing these broader risks are listed in Annex C.

4.8 It should be noted that NIS requirements do not apply directly to the supply chains of OES. It is the OES' responsibility to put in place appropriate and proportionate measures, and to ensure that their suppliers have in place appropriate measures, to manage risks of their services being disrupted via their supply chain.

NIS incident notification

4.9 The NIS Regulations also make it mandatory to notify the Competent Authority of incidents affecting network and information systems that have a significant impact on the continuity of the essential service.

4.10 The way the UK has chosen to interpret this requirement is to make a distinction between:

- Reporting for incident management purposes (which, while strongly recommended, will continue on a **voluntary** basis); and
- **Mandatory** notifications under NIS Regulations (which are only required when the level of disruption caused by an incident meets a specified threshold).

4.11 We are making this distinction because we do not want OES to wait until an incident reaches the 'significant impact' threshold that the NIS Regulations require before seeking support from the NCSC and other parts of Government in containing and mitigating incidents that risk affecting essential services.

4.12 In summary, the mandatory incident notification requirements under the NIS Regulations sit alongside any voluntary or existing mandatory reporting requirements to support incident response. The purpose of notifications under the NIS Regulations is to enable Competent Authorities to take any necessary regulatory follow-up actions and to meet other national obligations in the Directive, such as cross-border coordination. In general, we would still expect all organisations, including OES, to voluntarily report any significant cyber incidents to the NCSC (in the first instance) and DfT so they can get support and assistance on managing the incident and so that Government can also respond effectively when required.

Incident notification requirements

4.13 The NIS Regulations require OES to notify the Competent Authority of incidents **without undue delay and no later than 72 hours after the OES is aware that a notifiable incident has occurred.**

4.14 A notifiable incident is any incident which **has an actual adverse effect on the security of network and information systems** and **results in an impact on the**

continuity of the essential service that meets the thresholds set out in Annex E[1,2].

4.15 'Security of network and information systems' is defined in the NIS Regulations as the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

4.16 Early notification is strongly encouraged. Where an incident has not yet met the threshold but it is likely or expected that it might meet the threshold at a future point, it should be reported as soon as possible.

4.17 Should a NIS incident occur that affects multiple OES, all impacted OES are required separately to notify the incident to the relevant Competent Authority. If an OES is in any doubt over whether it needs to notify the relevant Competent Authority of an incident, the OES is encouraged just to do so.

Who to notify and what information is required

Mandatory notifications under NIS Regulations

4.18 All incidents that meet the thresholds set out in Annex E must be notified to the relevant Competent Authority as listed in Table 1.

4.19 Where the relevant Competent Authority is the Secretary of State for Transport, all notifications should be submitted to the DfT Cyber Compliance Team (CCT). Where the Secretary of State for Transport is not the Competent Authority (e.g. in relation to rail and roads in Northern Ireland), OES should refer to advice from the relevant Competent Authority. For the aviation sector, where both the Secretary of State for Transport and the Civil Aviation Authority are acting as the Competent Authority for the UK, notifications should still be submitted to the CCT who will then share them with the Civil Aviation Authority.

4.20 An incident notification template can be found in Annex F which details the information that should be submitted to the CCT. Contact details for reporting have been provided to all OES. The team will log the incident and decide what follow-up investigation is required.

4.21 The CCT does not have a specific responsibility for incident response[3].

Voluntary reporting to Government

4.22 For cyber incident response purposes, whether a NIS incident or not, all OES should still follow the voluntary incident reporting guidance which has been issued to operators within the transport sector.

Incident response

4.23 Aside from the NIS Regulations, DfT would also like to clarify how cyber security incidents are managed in the UK and to reiterate what information the NCSC and

[1] These thresholds only apply to OES where the relevant Competent Authority is the Secretary of State for Transport or the Civil Aviation Authority.
[2] It should be noted that the Regulations also include the requirement to report significant disruption to the essential service (i.e. that meets the thresholds) caused by an incident affecting any Digital Service Provider in scope of the Regulations (e.g. cloud service providers).
[3] Whilst the Cyber Compliance Team do not themselves have responsibility for incident response, DfT does have this responsibility and the capability resides with the Transport Security Operations Centre (TSOC) and other transport security policy teams within the Department. The DfT will work closely with the NCSC, other Government Departments (if required) and the National Crime Agency (for cyber-crime) on the response to cyber incidents affecting the transport sector.

other parts of Government should receive. Incident response to cyber security incidents under the NIS Regulations will remain the same as with any significant cyber security incidents affecting the transport sector. The response within Government for a cyber incident that impacts on transport is the responsibility of the NCSC, DfT, wider Government departments (if required) and the National Crime Agency (NCA) for cyber-crime. These organisations work closely together on cyber incident response but also on wider policy issues. Further information on all of these can be seen in Table 2 below.

4.24 It is essential that the NCSC and DfT receive timely reports from transport sector organisations on any major cyber security incidents. This reporting enables transport operators to get appropriate support and assistance on incident response and remediation, and to obtain additional context around incidents from the NCSC which they may have from various information sources. For Government this reporting is important to enable authorities to (i) build an informed understanding of the threats affecting UK industry; (ii) to share advice across sectors where appropriate; (iii) to enable specific law enforcement responses where required; and (iv) to provide links to and coordinate other Government and wider stakeholders, including coordinating and aligning communications and wider messaging to sectors.

4.25 DfT has developed and issued bespoke guidance for OES and other CNI operators explaining how to submit voluntary cyber security incident reporting to the NCSC (or Action Fraud) and DfT, which sits alongside NIS mandatory reporting requirements for OES.

Department for Transport (DfT)	DfT is the Lead Government Department (LGD) for any cyber incidents that impact on the transport sector. DfT will lead on the management of real-world operational impacts and provide the wider policy response. Our dedicated Transport Cyber Security team is also able to provide guidance and support as required.
National Cyber Security Centre (NCSC)	The NCSC is the UK's technical authority on cyber security. Its main purpose is to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience. It works with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management, underpinned by world class research and innovation. The NCSC identifies and responds to incidents which might impact the UK's national security or economic wellbeing, and/or which have the potential to cause major impact to the continued operation of an organisation. In the event of significant cyber security incidents, it provides direct technical support and cross-Government coordination of response activities.
National Cyber Crime Unit (NCCU)	The NCCU, part of the NCA, is the UK's lead for tackling the threat from serious and organised cyber-crime. The NCCU leads, supports and coordinates cyber law enforcement activity across the UK, working with partners to provide specialist cyber support and expertise across law enforcement. It works closely with the NCSC, Regional Cyber Crime Units and Police Forces to build an effective cyber response across the UK.
Action Fraud	Action Fraud is the UK's national fraud and cyber-crime reporting centre for England, Wales and Northern Ireland, providing a central point of contact for citizens and businesses. The National Fraud Intelligence Bureau (NFIB), also hosted by the City of London Police (CoLP), acts upon the information and crimes reported to Action Fraud, developing and disseminating crime packages for investigation locally, regionally and nationally, and executing a range of disruption and crime prevention techniques for victims across all sectors to target criminality and engineer out the threat from fraud and cyber-crime.

Table 2 Cyber incident response within Government

4.26 Incident response for broader resilience events affecting network and information systems (i.e. those that are not cyber attacks) in the transport sector will be the responsibility of DfT as the Lead Government Department, as with any other type of incident that causes significant disruption to transport services whether related to security or wider resilience issues. OES should therefore continue to report such incidents to DfT following any existing regulatory requirements and guidance.

4.27 For security, this includes examples such as the UK Maritime Security Measures under the International Ship and Port Facility Security Code (ISPS), the National Aviation Security Programme (NASP), Mandatory Occurrence Reports (MoRs) under EU Regulation 376/2014, rail security regulation and any existing reporting agreements with DfT.

4.28 For other no-notice incidents, such as any broader resilience issues causing disruption (e.g. severe weather), DfT has well-established links with relevant stakeholders within each sector and will work closely with them to keep up to date on the latest information.

Identification of relevant network and information systems by OES

4.29 When identifying the specific network and information systems that NIS security requirements apply to, OES should have regard to the specific essential service they provide. The security requirements only apply to the network and information systems being used in support of delivering an essential service and where it is assessed that the compromise of such a system could result in an impact on the continuity of the essential service.

4.30 To support this process, the following provides more clarity on what is considered to be the essential service for each of the entities specified in Annex D.

4.31 **Aviation: Airports, air navigation service providers and air carriers**

Provision of safe and secure services and facilities that enable: a) aircraft to land and take off at airports without undue delay or disruption, and b) passengers to depart and arrive without undue delay or disruption. For example, this could include, but is not limited to, check-in facilities, departure control services, security of passengers and baggage, air navigation services (including en-route) and aircraft operation.

4.32 **Maritime: Harbour authorities, operators of port facilities, operators of vessel traffic services and shipping companies**

For ports, the essential service will be reflected in whichever specific threshold that port meets. For example, if a port meets the threshold of having more than 10 million passengers per year, and does not meet any of the other thresholds, then the essential service is passenger transport. If a port meets more than one threshold, such as more than 10% of total UK liquid bulk and more than 15% of total UK lift-on lift-off freight, then movement of those freight types is the essential service. In all cases this includes enabling the ships to berth, load/unload and unberth, as well as moving the passengers/freight through the port. This may include, but is not limited to, operation of port facilities (also captured separately as OES), pilotage and operation of vessel traffic services (also captured separately as OES).

For shipping companies, the essential service is provision of safe and secure freight and passenger transport services without undue delay and disruption and such that the port can continue with the provision of its essential services as described above.

4.33 **Rail: Operators of rail assets for domestic, international and light rail/metro/underground**

The essential service provided by all the rail OES in scope is to enable the safe and secure movement of passengers and freight by rail without undue disruption or delay.

4.34 **Roads: Roads authorities**

The essential service is to ensure the effective operation of the road network and to seek to minimise disruption to road users that might reasonably be expected to occur as a result of unplanned disruption to the network.

5. Competent Authority approach

5.1 The approach outlined in this section applies where the Competent Authority is the Secretary of State for Transport or, in the case of aviation, the Secretary of State for Transport and the Civil Aviation Authority. Where this is not the case, OES should refer to advice from the relevant Competent Authority.

Overall approach

5.2 Competent Authorities are required to monitor the application of the NIS Regulations, which includes monitoring whether OES are meeting their security duties. This will be done through assessing the level of compliance of OES against the security requirements set out in section 4 of this document. This role must be fulfilled through a proactive approach which specifically includes direct engagement with OES, publishing guidance (such as this document) and implementing an assessment framework to check compliance with the security requirements which includes an audit regime. The overarching principle of this process is one of collaboration between Competent Authorities and OES.

5.3 The approach that the DfT Cyber Compliance Team (CCT) intends to use for the maritime, rail and roads sectors will be to conduct assessments using the Cyber Assessment Framework (CAF) published by the NCSC. The CAA has developed an aviation sector-specific assessment framework which will be used for the aviation sector (further information on this can be found in section 6 of this document).

5.4 Please note, that while DfT and CAA have discretion over many aspects of implementation of the Directive across transport, there are a number of key elements that have been determined on a national basis and to support specific requirements of the Directive that we are legally bound to apply.

5.5 OES are advised to nominate a point of contact within the organisation with whom the DfT and the CAA can communicate information concerning the NIS Regulations.

Expectations within the first year

5.6 All OES are expected to complete self-assessments using the relevant assessment frameworks in the first instance. It is expected this self-assessment process will take a number of months for OES to complete and achievable deadlines have been set. Over the period of self-assessment, OES are expected to engage directly with the CCT/CAA, and to raise any queries they have on how to apply the assessment. See section 6 for further details of the CAA assessment framework for the aviation sector.

5.7 Upon completion of the self-assessment, the results will be discussed with the CCT/CAA. Using the results of the assessments, the CCT/CAA will work with OES to establish if and when improvements should be made. OES will need to propose

what measures they consider appropriate and it will be for the CCT/CAA to determine whether they are sufficient.

5.8 It may be determined by the CCT/CAA that more evidence is required to support the self-assessment. In these cases OES may be instructed to appoint an independent third party to conduct an audit. These could be general audits covering all areas of the CAF or CAP 1574 (for aviation – see section 6) or could focus on specific areas of concern that have been identified in the self-assessment and through subsequent engagement. Where audits are required, it will be the responsibility of the OES to contract the third party from a list of suitably qualified organisations provided by CCT or the CAA and the intention is that OES pay the costs.

5.9 Beyond the first year, the CCT and the CAA will use the results of the self-assessment, along with threat and vulnerability information, to establish a risk-based programme of ongoing activity (including audits as described above) to monitor compliance. Action will be focussed on organisations where the most serious concerns have been identified and/or where potential incidents could have the greatest impacts on the sector. The exact nature of this activity may differ between OES and timescales will be agreed. Alongside this focussed activity, all OES should strive to improve the security of their network and information systems, following the NIS Regulations, principles and assessment frameworks.

Stepped approach to enforcement

5.10 The CCT/CAA will use a stepped approach to enforcement when an OES is found to be failing to meet requirements. This relies heavily on a collaborative approach between the CCT/CAA and OES. Any enforcement, particularly the issuing of penalties, will be a last resort and in all cases will be proportionate to the failing identified.

5.11 The stepped approach that will be taken in the transport sector can be summarised as follows:

Step 1: Advise and persuade

- When any deficiencies are identified, the initial approach taken by the CCT/CAA will be to engage and discuss this with the OES. This will include discussing what the failing or deficiency is and how and when it can be addressed. The CCT/CAA will agree the remedial actions proposed by the OES and when these actions should be completed. The CCT/CAA may wish to follow-up with further assessments or audits to ensure that these actions have been taken and any failings have been addressed appropriately and proportionately.
- A stronger line may be taken if these actions fail to be addressed in the agreed timeframe although this can still stop short of any formal enforcement action.
- The CCT/CAA may issue information notices requiring the OES to provide specified information to support compliance assessment.

Step 2: Enforcement notice

- Where the initial collaborative approach has not worked and it is clear that failings are not being addressed, a formal enforcement notice will be issued. This will set out the failings identified, the steps to be taken and the time period in which they need to be completed.

Step 3: Penalty notice

- Where the OES has failed to take adequate steps to rectify a failure identified in an enforcement notice a monetary penalty may be issued. In practice such a step is likely to be taken only in extreme cases and as a last resort where the initial actions taken by the CCT/CCA have not been successful at instigating action by the OES.
- In determining the value of the monetary penalty, the CCT/CAA will consider the appropriate and proportionate level within the prescribed limit of £17m.

5.12 Compliance regimes for DfT's other security regulations will continue in parallel with this approach.

5.13 Note that we also cannot rule out the possibility that enforcement action could be taken under both the General Data Protection Regulation (GDPR) and NIS Regulations because these are separate legislative regimes with differing legal requirements. This will apply not just to GDPR but other sectoral and general legislation. Note, however, that the NIS Regulations make provision, at regulation 23, for Competent Authorities to consider whether enforcement action is reasonable and proportionate on the facts and circumstances of the case, including consideration of whether a contravention is also liable to enforcement under another enactment.

5.14 It should also be noted that regulation 19 of the NIS Regulations sets out a process for OES to request independent review of penalty decisions taken by the Competent Authority.

Incident investigation – approach that will be taken following an incident

5.15 As has been set out in section 4 of this document, all OES must notify the CCT of incidents that meet the designated thresholds. Following the notification, and allowing for a period of resolution and recovery, the CCT/CAA will decide whether or not the incident requires further follow-up investigation. This may include requesting further details of the incident.

5.16 The purpose of these investigations could be to: i) establish the cause of the incident and assess whether the incident was preventable; ii) assess whether effective and reasonable risk management was in place; iii) assess whether the operator had appropriate security measures in place; and iv) assess how the OES responded to and managed the incident.

5.17 Once the investigation has concluded, the CCT/CAA will decide on any appropriate next steps, be it no action, advice or formal enforcement action.

5.18 It is expected that OES will also conduct their own investigations and this will form the basis for the conversation between the CCT/CAA and the OES. The CCT/CAA may require additional information and in some cases may instruct the OES to appoint a third party investigator and/or auditor from an approved list. Where these are required, our intention is that it will be the responsibility of the OES to contract the third party and pay the costs. The results of such investigations/audits should be shared with the CCT/CAA to determine if further action is required.

5.19 It should be noted that simply having an incident is not in itself an infringement of the NIS Regulations and therefore does not automatically mean enforcement action

will be taken. The key factor for determining whether enforcement action should be taken when there has been an incident, is whether or not appropriate and proportionate security measures and procedures were in place and being followed. This will come from the post-incident investigation conducted by the CCT/CAA. Not having notified the Competent Authority of an incident that meets the incident notification thresholds would be an infringement of the NIS Regulations.

6. Aviation sector guidance

DfT and CAA roles/responsibilities

6.1 DfT and the CAA are both acting as Competent Authority for the aviation sector and there is a clear division of roles and responsibilities between the two organisations. In summary, the CAA will be the primary organisation with which the OES in the aviation sector will engage on a regular basis and it is intended that the Secretary of State for Transport will only be formally involved when enforcement action is required. Incident notifications will also be submitted to the DfT CCT.

6.2 The CAA will be responsible for ensuring that the aviation sector meets the requirements of the NIS Regulations through proactive engagement, as well as carrying out assessments and audits. The CAA will be responsible for working with OES to agree how and when any deficiencies are addressed and to follow up to ensure actions are taken. The CAA will also be responsible for post-incident investigation.

6.3 Decisions to take formal enforcement action will be the responsibility of the Secretary of State for Transport (i.e. issuing enforcement notices or penalty notices). The CAA will provide advice to the Secretary of State for Transport with a recommended course of action based on its compliance assessments and engagement with the OES. However, decisions on enforcement will rest with the Secretary of State for Transport.

6.4 A breakdown of each of the roles and responsibilities of the Competent Authority and who is responsible can be found in Table 3 below.

Role of Competent Authority	Who is responsible?	Background
Reviewing the application of the NIS Regulations in their sector or region (see section 5)	CAA	It will be the responsibility of the CAA to ensure that OES within the aviation sector are meeting the requirements of the NIS regulations which will include proactive engagement with the sector and managing the assessment and audit programme.
Establishing identification thresholds for OES in their sector or region (see section 3) including keeping a list of all OES who are designated and all revocations	Secretary of State for Transport (on advice from CAA)	Whilst DfT have been responsible for setting the thresholds for OES it will be the ongoing responsibility of the CAA to ensure that organisations meeting these thresholds are identified.
Assessing compliance of OES with the requirements of the NIS Regulations, including audits (see section 5)	CAA	The CAA will be responsible for assessing compliance of all aviation OES with the requirements in the NIS Regulations. The CAA will be responsible for instructing OES to complete the self-assessment and will be responsible for the audit programme.

		This includes requesting information from OES to support any compliance assessments. The CAA will also be responsible for agreeing with OES how and when any deficiencies should be addressed – this is prior to any formal enforcement action.
Investigating incidents (see section 5)	CAA	The CAA will be responsible for any follow-up investigations after incidents have occurred (although investigations will likely be conducted by approved third parties).
Cooperating with other Competent Authorities to provide consistent advice and oversight to OES or Digital Service Providers (see section 5)	CAA	It will be the responsibility of the CAA to ensure the approach taken in the aviation sector is consistent where possible with other sectors. This will include ensuring that CAA and DfT engage on the approach taken across the rest of the transport sector.
Enforcement (including issuing notices and penalties) of the requirements of the NIS Regulations (see section 5)	Secretary of State for Transport (on advice from CAA)	The decision to issue enforcement notices or penalties will rest with the Secretary of State for Transport. The CAA will provide advice to the Secretary of State for Transport and recommend action to take based on evidence from their compliance activities and engagement with OES but the decision on enforcement rests with the Secretary of State for Transport.
Preparing and publishing guidance to assist OES or Digital Service Providers in meeting the requirements of the NIS Regulations (includes this guidance document)	Secretary of State for Transport	This will remain the responsibility of the Secretary of State for Transport, but the CAA will be asked to contribute to such guidance.
Determining the thresholds for notifiable incidents in their sectors or regions (see section 4)	Secretary of State for Transport	This will remain the responsibility of the Secretary of State for Transport although input and agreement will be sought from the CAA on thresholds for the aviation sector.
Receiving incident notifications (see section 4)	Secretary of State for Transport	The Secretary of State for Transport will remain the primary recipient of incident notifications although any notifications received will be shared with the CAA which will be responsible for any follow-up actions taken.
Making sure that there are processes in place for incident response for other types of incidents (i.e. those that are not a cyber attack) and issuing guidance to support companies dealing with those types of incidents (see section 4)	Secretary of State for Transport	This will be the responsibility of the Secretary of State for Transport although incident response for these types of incidents will be managed in the same way as any wider resilience or physical security issue.

Table 3 Split of Competent Authority roles and responsibilities between the CAA and Secretary of State for Transport

CAP 1574 and the CAA assessment framework

Introduction to CAP 1574

6.5 The CAA has developed CAA Publication, *CAP 1574: Twenty-six security controls for regulation*. CAP 1574 details twenty six cyber security controls which provide a framework for the management of cyber-induced risks within the aviation industry, primarily in respect of aviation safety. The CAA later conducted an assessment of the controls against the NIS principles and concluded the controls appropriately supported the delivery of NIS.

6.6 CAP 1574 was developed to assist aviation organisations in meeting both the requirements under the NIS Regulations and their European Aviation Safety Agency (EASA) safety obligations, by assessing their management systems. It includes the control measures considered by the CAA to cover the requirements of the NIS Regulations as far as they relate to cyber security. It includes a diagram that shows the relative order of the assessment and the increased dependence on external factors or collaboration.

6.7 To help OES in assessing their conformity with CAP 1574, the CAA has developed a self-assessment tool.

Relationship to the CAF

6.8 As described in section 2, the NCSC has developed the Cyber Assessment Framework (CAF). The CAF is intended to be a systematic method for assessing the extent to which OES are achieving the outcomes specified by the NIS principles.

6.9 The CAF is designed to be used by OES within all sectors whereas CAP 1574 is aviation-focused. CAP 1574 assessment tool is an objective assessment based on several questions on each principle that allows the organisation to answer a specific closed question. The answer they give informs a system that develops an automatic results summary.

6.10 The CAA has determined that, as CAP 1574 effectively covers the NIS requirements whilst also accounting for the specialist nature of many systems in the aviation sector, this tool should be used as the primary measure of compliance by OES.

6.11 CAA's cyber specialists have reviewed both documents in order to ensure maximum interoperability between CAP 1574 and the CAF and prevent any conflicts arising. In the course of developing CAP 1574 CAA sought and received an endorsement for its approach from the NCSC. Additionally, the NCSC will review CAA's proposed assessment tool to ensure there are no conflicts with the CAF.

Assessing and assuring compliance

6.12 The assessment of OES compliance by the CAA Cyber Oversight Team will be carried out in two phases as detailed below.

Initial assessment (Phase 1)

6.13 Phase 1 involves OES using the assessment tool developed by the CAA Cyber Oversight Team. The tool provides high-level results allowing OES to quickly identify those systems that may have a larger risk exposure or need urgent rectification action and to prepare for Phase 2 Oversight.

6.14 OES will be specifically required to complete an assessment using the tool and share results with the CAA. This tool will comprise two parts:

- Part 1: High-level questions intended to identify an entity's general cyber readiness and governance; and
- Part 2: Focused questions that address the elements of CAP 1574 as they relate to the systems which have been identified as essential under NIS Regulations.

6.15 The high-level questions in part 1 will require OES to answer a set of questions aimed at identifying NIS critical systems, gaining an understanding of the governance, cyber hygiene and the level of independent assurance entities may have already sought. This will be returned to the CAA ahead of the second part of the assessment.

6.16 Part 2 will comprise a series of closed questions grouped under each of the 26 controls described in CAP 1574. Delivered through a prepopulated spreadsheet, when answered, these will build a results summary for the OES. This results in a tactical assessment of individual critical systems or groups of systems. It is not aimed at providing a strategic assessment for the organisation as a whole. The CAA's approach mirrors that required for all Competent Authorities and OES but adopts an aviation-specific approach. Additionally, this allows the OES to 'gain credit' by accounting for those systems which are already independently certified or monitored as meeting international cyber security standards. An example of the assessment is shown in Figure 1.

CAA Cyber Security Self-Assessment Questionnaire

Organisation:	Aviation Company and/or Entity UNID
Systems assessed:	System A, B & C
Assessor:	Name & role of assessor
Date:	01 January 2018
Risk Tolerance:	Medium

Summary: 26 / 0 / 0

9	Controlled Access	9.1	Users are only permitted access to networks and information systems that are required for their role.	N	Improve	Role-Based Access Control (RBAC) or a manual authorisation process should be evidenced.
		9.2	The level of access to information and functions for critical systems is based on essential need only.	N		It should be demonstrated that the level of access is commensurate with the roles performed by individual users.
		9.3	Regular audits are conducted to ensure that only essential personnel have access to critical aviation systems.	N		Evidence of regular audits should be available. The recommended frequency is no less than four times per year. Should include reviews of usage logs to identify dormant accounts.
		9.4	Formal revocation procedures ensure that access to a system is revoked immediately it is no longer required.	N		Evidence recent revocation examples, i.e. access has been removed for previously authorised users who no longer require that access.

Figure 1 Example of CAA cyber security questionnaire

Oversight (Phase 2)

6.17 To support OES in achieving the independent validation of their responses outlined in Phase 1, the CAA proposes to develop an overarching framework of accredited testers and auditors against a series of cyber security competencies. This will allow OES, when undertaking validation of the outcomes of their initial assessments, to draw upon independent, properly qualified resources.

6.18 The CAA is currently working to establish these frameworks and lists of appropriately qualified third parties. Further details will be provided in advance of OES progressing to Phase 2.

6.19 The outcomes of these assessments, audits and tests should be structured into a single report, to be shared with the CAA, outlining how the OES proposes to rectify any gaps in compliance which have been found in either phase. The CAA will monitor the implementation of these plans as part of its oversight function.

7. Maritime sector guidance

NIS and the Maritime Codes of Practice and ISPS

7.1 The Institute of Engineering Technology (IET), in conjunction with the Department for Transport and the Defence Science and Technology Laboratory (Dstl), published the following documents:

- Code of Practice: Cyber Security for Ports and Port Systems (August 2016)
- Code of Practice: Cyber Security for Ships (September 2017)

7.2 These documents provide specific voluntary guidance on cyber security for the maritime sector. They use principles rather than national standards or legislation to promote good cyber security practice. They were designed to complement the existing requirements for ship and port facility security – specifically referencing the International Ship and Port Facility Security Code (ISPS Code) – by providing additional guidance on the cyber-related aspects of the security measures set out[4].

7.3 The Codes of Practice were published prior to the details of the UK implementation of the NIS Directive being established, and before the NCSC developed the 14 security principles. This section provides guidance on how the NIS Regulations and the NCSC's 14 principles align with the Codes of Practice and the ISPS Code.

7.4 In summary, all OES must comply with the NIS Regulations through meeting the 14 NIS principles. The NCSC has also published a suite of guidance to support OES in complying with these principles (as described in section 4). The NCSC guidance is intended to be generic guidance that can be applied to all sectors. The Codes of Practice provide an additional set of guidance that may be used by OES in the maritime sector to support compliance with some elements of the NIS requirements.

7.5 There is no specific conflict between the Codes of Practice and the NIS principles. If organisations have been following the Codes of Practice then they will be making progress towards complying with the NIS principles. The Codes continue to provide a range of useful information and guidance on cyber security that is specific to the maritime operational environment. However, it is important to note that although there is overlap in a number of areas, following the Codes of Practice and the ISPS Code will not automatically make an organisation compliant with the NIS Regulations. The Codes should only be considered as additional supporting guidance and were never intended to be legally binding. The NIS principles go further than the Codes and there is additional technical guidance that has been developed by the NCSC that is not reflected in the Codes.

7.6 Ultimately, the NIS security principles are outcome-based and it is for OES to decide how they want to achieve them in the context of their organisation and in

[4] The ISPS Code contains measures to enhance the security of ships and port facilities and is mandatory for the contracting governments to the Safety of Life at Sea Convention.

agreement with the Competent Authority. An organisation may wish to align their NIS compliance with the ISPS Code in areas where it makes sense to do so (for example aligning relevant governance and risk assessment requirements). Similarly, an organisation may choose to follow elements of the relevant Code of Practice to support their compliance in areas where they provide a complementary sector-specific perspective. As far as the NIS Regulations are concerned, DfT will look to assess that the security outcomes the NCSC have defined are being adhered to, rather than specifying a particular method of achieving them.

7.7 The following sections are intended to illustrate where the Codes of Practice may provide some sector-specific detail that is helpful and complimentary to the NCSC guidance, and where there are linkages to the ISPS Code that might be useful when considering how to meet the objectives in the NIS principles.

Objective A: Managing security risk

A.1 Governance

- ISPS Code Part A established a requirement for ship security officers, company security officers (for shipping companies) and port facility security officers.
- Section 6.1 of the Ports Code of Practice and section 7.1 of the Ships Code of Practice covers the roles of the Cyber Security Officer (CySO) and Company Security Officer (CSO).

A.2 Risk management

- ISPS Code Sections B 8.3 and 15.3[5] established a requirement for a port facility security assessment and ship security assessments to take account of cyber security.
- ISPS Code section 3.2, together with sections 4 and 5 of the Ports Code of Practice and sections 5 and 6 of the Ships Code of Practice (with further detail in the appendices) cover risk management in the context of developing a cyber security assessment and cyber security plan.

A.3 Asset management

- ISPS Code Part A requires asset identification as part of a port facility security assessment (PFSA).
- Section 4.1 and Appendix B1 in the Ports Code of Practice contain maritime specific information.
- Section 5 and Appendix B1 in the Ships Code of Practice contain maritime specific information.

A.4 Supply chain

- The Codes of Practice provide some sector-specific guidance. It is covered in sections 5 and 6 and appendices A and C of the Ports Code of Practice. The Ships Code of Practice has a separate appendix on supply chain security: Appendix G.

[5] Mandatory within the EU by virtue of EC Regulation 725/2004.

Objective B: Defending systems against cyber attack

B.1 Service protection policies and processes

- Please follow section B.1 of the NIS guidance.
- Sections 4, 5 and 6 of the Ports Code of Practice and sections 5, 6 and 7 of the Ships Code of Practice provide some specific information on developing a cyber security assessment, cyber security plan and managing cyber security.

B.2 Identity and access control

- Please follow the NIS guidance.
- Appendix D of the Ships and Ports Codes of Practice, specifically D1 and D2, provide some guidance on people and physical control.

B.3 Data security

- Please follow the NIS guidance.

B.4 System security

- Please follow the NIS guidance.

B.5 Resilient networks and systems

- Section D5 of both Codes of Practice provides some high level guidance on resilience.

B.6 Staff awareness and training

- Please follow the NIS guidance.

Objective C. Detecting cyber security events

C.1 Security monitoring

- Please follow the NIS guidance.

C.2 Proactive security event discovery

- Follow the NIS guidance as limited information in the Codes of Practice. Detection is mentioned in section 6.3 and Appendices D.3 and D.5 of the Ports Code of Practice and section 7.2 and Appendices D.3, D.5 and G of the Ships Code of Practice.

Objective D. Minimising the impact of cyber security incidents

D.1 Response and recovery planning

- The NIS guidance provides more detailed information than Codes of Practice. Response planning is covered in sections 6 and 7 of both Codes of Practice. Appendix G of the Ports Code of Practice and Appendix F of the Ships Code of Practice cover incident handling.

D.2 Lessons learned

- The NIS guidance provides more detailed information than the Codes of Practice. Appendix G of the Ports Code of Practice and Appendix F of the Ships Code of Practice briefly cover lessons learned.

The following table provides an analysis of the NIS principles which have been cross-referenced against the Codes of Practice for both Ports and Ships:

NIS Principles	Code of Practice: Cyber Security for Ports and Port Systems	Code of Practice: Cyber Security for Ships
A1 Governance	Section 6.1 (also see ISPS Code Part A)	Section 7.1 (also see ISPS Code Part A)
A2 Risk management	Sections 4 and 5 (also see ISPS Code section B 8.3 and 15.3)	Sections 5 and 6 (also see ISPS Code section B 8.3 and 15.3)
A3 Asset management	Section 4 and Appendix B1	Section 5 and Appendix B.1
A4 Supply chain	Sections 5,6 and Appendices A and C	Appendix G
B1 Service protection policies and processes	Section 4,5 and 6	Section 5, 6 and 7
B2 Identity and access control	Appendices B and D	Appendices B and D
B3 Data security	Appendix D	Appendix D
B4 System security	Appendix D	Appendix D
B5 Resilient networks and systems	D5	n/a
B6 Staff awareness and training	Brief coverage in section 6 and Appendices C, D and E	Brief coverage in Appendices C, D and G
C1 Security monitoring	n/a	n/a
C2 Anomaly detection	Brief coverage in section 6.3 and Appendix D	Brief coverage in section 7.2 (includes schematic of a SOC) and Appendices D and G
D1 Response and recovery planning	Sections 6 and 7, Appendix G	Sections 6 and 7, Appendix F
D2 Lessons learned	Appendix G	Appendix F

Table 4 Cross-reference of NIS principles with Codes of Practice

8. Rail sector guidance

8.1 The rail sector is regulated for security under the Railways Act 1993 and the Channel Tunnel Security Order 1994. Many organisations identified as OES in the rail sector will be in scope of existing rail security regulation and will have to comply with cyber security requirements.

8.2 The following guidance summarises how OES should approach the requirements of the NIS Regulations and the requirements within existing rail security regulation.

8.3 Broadly, the NIS Regulations will require more from operators than current rail security regulation. The NIS Regulations will require action from all operators that are in scope to apply appropriate and proportionate security measures in line with the NIS principles and guidance to protect network and information systems that support the delivery of essential services.

8.4 Existing rail security regulation is designed to protect the rail network from "acts of violence" (which is defined in legislation). The NIS Regulations have a slightly broader purpose to protect against a wider range of threats (security and wider resilience hazards). They are not constrained to protecting only against acts of violence, but cover acts that could result in consequences that are disruptive to the essential service but may not necessarily meet the legislative definition of acts of violence.

8.5 However, there are significant overlaps between the NIS Regulations and current rail security regulation on issues such as governance, risk management, asset management, supply chain, staff awareness and training, response and recovery planning and improvement. In areas where there is overlap if an organisation is complying with the NIS Regulations it will, by default, also comply with current rail security regulation.

8.6 The NIS Regulations and the current rail security regulation differ in some areas such as incident reporting. OES should be aware of the differences in the types of events in scope for reporting, reporting thresholds and reporting timeframes. If in doubt about reporting an incident, it should be reported to all relevant parties or clarification should be sought.

8.7 It is very likely that the systems in scope of rail security regulation and the NIS Regulations will be the same. However, this will depend on whether operators deem that systems in scope for rail security regulation are critical for the operation of an essential service and so identify them under NIS requirements.

8.8 It is important to note that not all organisations will be in scope of both the NIS Regulations and rail security regulation. Although the majority of rail organisations should expect to be so, for a small number only one of the regimes will apply.

9. Roads sector guidance

9.1 Unlike aviation, maritime and rail, the roads sector is not subject to existing regulations or requirements that cross over with the NIS Regulations. Those OES within scope of the NIS Regulations for the road sector should work within their existing licencing agreements (or similar) on any areas affecting the security of network and information systems, as well as complying with the NIS Regulations.

Annex A: Key documents

The following table contains a list of the key documents referenced in this guidance.

Document and description	**Hyperlink**[6]
EU Directive 2016/1148 on the security of network and information systems (NIS Directive) *Full text of the NIS Directive (in PDF format)*	http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
Network and Information Systems Regulations 2018 *Full text of the Statutory Instrument that transposes the NIS Directive into UK law*	https://www.legislation.gov.uk/uksi/2018/506/contents
Consultation on the Security of Network and Information Systems Directive *Details of the public consultation run by DCMS and the Government response that determined how the UK would implement the Directive*	https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive
NCSC's NIS Guidance Collection *This is the central page linking to all of the NCSC's guidance on the NIS Directive*	https://www.ncsc.gov.uk/guidance/nis-guidance-collection
Top-level NIS objectives and NCSC guidance *This page lists the four top-level security objectives that the UK is using to implement article 14 of the NIS Directive, linking through to the principles and guidance for each area*	https://www.ncsc.gov.uk/guidance/nis-directive-top-level-objectives
Table view of the 14 principles and related guidance *Summary of the 14 NIS principles and their related external guidance*	https://www.ncsc.gov.uk/guidance/table-view-principles-and-related-guidance

[6] Hyperlinks correct as of 3rd December 2018.

Cyber Assessment Framework (CAF) *Assessment tool developed by the NCSC to aid OES compliance with the security principles*	https://www.ncsc.gov.uk/guidance/cyber-assessment-framework-caf
CAP 1574 *Controls framework developed by the CAA to regulate cyber-induced risks within the aviation industry. OES in aviation will be assessed against these controls.*	http://publicapps.caa.co.uk/docs/33/26%20security%20controls%20for%20regulation_V4.pdf

Table 5 List of key documents

The following table lists a number of other relevant documents referenced in this guidance.

Document	Hyperlink[7]
Code of Practice: Cyber Security for Ports and Port Systems	https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice
Code of Practice: Cyber Security for Ships	https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice

Table 6 List of related documents

[7] Hyperlinks correct as of 3rd December 2018.

Annex B: The NIS security principles

The implementation of Article 14 of the NIS Directive is described via 4 top-level objectives. The objectives will be realised through implementation of 14 sector-agnostic security principles devised by the NCSC. Each principle describes mandatory security outcomes to be achieved. The full guidance collection on the NCSC's website (see Annex A) goes into further detail on each principle with references to a range of existing guidance and standards.

Objective A: Managing security risk

Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.

A1. Governance

Putting in place the policies and processes which govern your organisation's approach to the security of network and information systems.

A2. Risk management

Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management.

A3. Asset management

Determining and understanding all systems and/or services required to maintain or support essential services.

A4. Supply chain

Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers.

Objective B: Protecting against cyber attack

Proportionate security measures are in place to protect essential services and systems from cyber attack.

B1. Service protection policies and processes

Defining and communicating appropriate organisational policies and processes to secure systems and data that support the delivery of essential services.

B2. Identity and access control

Understanding, documenting and controlling access to essential services systems and functions.

B3. Data security

Protecting stored or electronically transmitted data from actions that may cause disruption to essential services.

B4. System security

Protecting critical network and information systems and technology from cyber attack.

B5. Resilient networks and systems

Building resilience against cyber attack.

B6. Staff awareness and training

Appropriately supporting staff to ensure they can support essential services' network and information system security.

Objective C: Detecting cyber security events

Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.

C1. Security monitoring

Monitoring to detect potential security problems and track the effectiveness of existing security measures.

C2. Proactive security event discovery

Detecting anomalous events in relevant network and information systems.

Objective D: Minimising the impact of cyber security incidents

Capabilities to minimise the impact of a cyber security incident on the delivery of essential services including the restoration of those services where necessary.

D1. Response and recovery planning

Putting suitable incident management and mitigation processes in place.

D2. Lessons learned

Learning from incidents and implementing these lessons to make a more resilient service.

Annex C: Broader resilience risks to network and information systems

The following are examples of existing guidance and standards that include elements related to broader resilience risks to network and information systems which OES may find helpful.

C.1 **CPNI website**

https://www.cpni.gov.uk/network-and-information-systems-nis

A useful resource for all organisations is the CPNI website which contains advice and guidance on many aspects of physical and personnel security.

C.2 **Technical guidelines for the implementation of minimum security measures for Digital Service Providers**

https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

This document was produced by the European Union Agency for Network and Information Security (ENISA) to define the common baseline security objectives for DSPs under the NIS Directive. It describes different levels of sophistication in implementing those objectives and maps the objectives against other well-known industry standards, guidance and frameworks.

Whilst this has been developed for DSPs there are sections that are also relevant to OES. It contains two sections specifically on managing broader resilience risks:

- SO 08 – Physical and environmental security

The DSP establishes and maintains policies and measures for physical and environmental security of data centres such as physical access controls, alarm systems, environmental controls and automated fire extinguishers etc.

- SO 09 – Security of supporting utilities

The DSP establishes and maintains appropriate security measures to ensure the security of supporting utilities such as electricity, fuel, HVAC etc. For example, this may be through the protection of power grid connections, diesel generators, fuel supplies, etc.

C.3 **ISO27001**

https://www.iso.org/standard/54534.html

This standard specifies the requirements for establishing, implementing and maintaining an information security management system. Section A.11 covers physical and environmental security.

C.4 NIST cyber security framework

https://www.nist.gov/cyberframework

This framework was developed by the US Government in collaboration with the private sector and contains a set of industry standards and best practice to support organisation in managing cyber risks. It was called for in a US Executive Order. The Framework Core is a set of cyber security activities, outcomes, and informative references that are common across critical infrastructure sectors. The following elements of the framework core provide some useful guidance and further references:

- PR.AC-2: Physical access to assets is managed and protected;
- PR.AT-5: Physical and information security personnel understand roles and responsibilities;
- PR.IP-5: Policy and regulations regarding the physical operating environment for organisational assets are met;
- DE.CM-2: The physical environment is monitored to detect potential cyber security events.

Annex D: Definitions and thresholds for identification of Operators of Essential Services

D.1 Identifying operators of essential services

Sub-sector	Essential service	Identification threshold
Air transport	Provision of services by the owner or manager of an aerodrome	Owner or manager of any aerodrome with annual terminal passenger numbers greater than 10 million. An "aerodrome" has the same meaning as in the Civil Aviation Act 1982.
	Provision of air traffic services (as defined in Transport Act 2000)	Any entity which is granted a licence by the Secretary of State or the Civil Aviation Authority to provide en-route air traffic services in the United Kingdom. An air traffic service provider at any airport which has annual terminal passenger numbers greater than 10 million.
	Provision of services by air carriers	An air carrier which has: a) more than 30% of the annual terminal passengers at any UK airport which has annual terminal passenger numbers greater than 10 million; and b) more than 10 million total annual terminal passengers across all UK airports. An "air carrier" has the same meaning as in Article 3(4) of Regulation (EC) No 300/2008.
Maritime transport	Shipping	A shipping company which handles- (a) over 5 million tonnes of total annual freight at UK ports; and (b) over 30% of the freight at any individual UK port which fulfils at least one of the following criteria – (I) it handles more than 15% of UK total roll-on roll-off traffic; (II) it handles more than 15% of UK total lift-on lift-off traffic; (iii) it handles more than 10% of UK total liquid bulk traffic; or (iv) it handles more than 20% of UK biomass fuel traffic; or A shipping company with over 30% of the annual passenger numbers at any individual UK port which has annual passenger numbers greater than 10 million.
	Provision of services by a harbour authority	A harbour authority (as defined in section 313(1) of the Merchant Shipping Act 1995) which - (a) has annual passenger numbers greater than 10 million; or (b) fulfils at least one of the following criteria: (i) it handles more than 15% of UK total roll-on roll-off traffic;

Sub-sector	Essential service	Identification threshold
		(ii) it handles more than 15% of UK total lift-on lift-off traffic; (iii) it handles more than 10% of UK total liquid bulk traffic; or (iv) it handles more than 20% of UK biomass fuel traffic.
	Provision of services by an operator of a port facility	(a) An operator of a port facility which handles passengers at a port which has annual passenger numbers greater than 10 million; or (b) An operator of a port facility at a port which fulfils at least one of the following criteria: (i) it handles more than 15% of UK total roll-on roll-off traffic; (ii) it handles more than 15% of UK total lift-on lift-off traffic; (iii) it handles more than 10% of UK total liquid bulk traffic; or (iv) it handles more than 20% of UK biomass fuel traffic; and where that port facility operator handles the same type of freight for which the port fulfils one of the criteria mentioned in sub-paragraphs (i)-(iv). "Port facility" has the same meaning as in regulation 2 of the Port Security Regulations 2009[8]
	Vessel traffic services	Operator of vessel traffic services at a port which- (a) has annual passenger numbers greater than 10 million; or (b) fulfils at least one of the following criteria: (i) it handles more than 15% of UK total roll-on roll-off traffic; (ii) it handles more than 15% of UK total lift-on lift-off traffic; (iii) it handles more than 10% of UK total liquid bulk traffic; or (iv) it handles more than 20% of UK biomass fuel traffic. "vessel traffic services" has the same meaning as in regulation 2(1) of the Merchant Shipping (Vessel Traffic Monitoring and Reporting Requirements) Regulations 2004[9]
Rail transport	Rail services in Great Britain	Any operator of a mainline railway asset but excluding operators of: i. railway assets solely for the provision of international rail services; ii. railway assets for metro, tram and other light rail (including underground) systems; iii. heritage, museum or tourist railways, whether or not they are operating solely on their own network iv. networks which are privately owned and exist solely for use by the infrastructure owner for its own freight operations or other passenger or freight services for third parties and operators of passenger or freight services on those networks (including high speed rail services). "Operator" has the same meaning as in section 6 of the Railways Act 1993. "Mainline railway" means all railways in Great Britain.

[8] SI 2009/2048
[9] SI 2004/2110

Sub-sector	Essential service	Identification threshold
		"Railway asset" has the same meaning as in section 6 of the Railways Act 1993. "International rail service" means a rail service where the train crosses the border of the UK and a Member State (an international border) and where the principal purpose of the service is to carry passengers or goods between stations located in the UK and stations in at least one Member State. The train may be joined and/or split, and the different sections may have different origins and destinations, provided that all carriages cross at least one international border.
	Railway services in Northern Ireland	Any railway undertaking in Northern Ireland. 'Railway undertaking' has the same meaning as in the Transport Act (Northern Ireland) 1967. The mainline railway network is defined to include all railways in Northern Ireland but excludes heritage railways operating solely on their own network.
	High speed rail services	Operator of a railway asset for high speed rail services. "operator" and "railway asset" have the same meaning as in section 6 of the Railways Act 1993.
	Metros, trams and other light rail (including underground) services	Operator of a railway asset for metros, trams and other light rail (including underground) systems with more than 50 million annual passenger journeys. "operator' and "railway assets" have the same meaning as in section 6 of the Railways Act 1993.
	International rail services	Any operator of a Channel Tunnel Train (as defined in the Channel Tunnel Security Order 1994). The infrastructure manager of the Channel Fixed Link (as defined in the Channel Tunnel Act 1987). "operator" has the same meaning as in section 6 of the Railways Act 1993. "International rail service" means a rail service where the train crosses the border of the UK and a Member State (an international border) and where the principal purpose of the service is to carry passengers or goods between stations located in the UK and stations in at least one Member State. The train may be joined and/or split, and the different sections may have different origins and destinations, provided that all carriages cross at least one international border.
Road transport	Road transport services	A road authority responsible for roads in the United Kingdom that annually in total have vehicles travelling more than 50 billion miles on them. "road authority" has the same meaning as in Article 2(12) of Commission Delegated Regulation (EU) 2015/962

Sub-sector	Essential service	Identification threshold
	Services provided by operators of Intelligent Transport Systems	A road authority that provides an Intelligent Transport Systems service that covers roads in the United Kingdom that annually in total have vehicles travelling more than 50 billion miles on them. "Intelligent transport system" has the same meaning as in Article 4(1) of Directive 2010/40/EU of the European Parliament and of the Council.

Table 7 Definitions and thresholds for identification of Operators of Essential Services

D.2 Statistics sources

Mode	Statistics source
Aviation	Annual airline and airport statistics published by the Civil Aviation Authority. https://www.caa.co.uk/Data-and-analysis/
Maritime	Annual UK Maritime and Shipping Statistics published by Department for Transport. https://www.gov.uk/government/collections/maritime-and-shipping-statistics#-data-tables For biomass: HMRC UKtradeinfo statistics https://www.uktradeinfo.com/Pages/home.aspx Commodity codes from Annex G to the Digest of UK Energy Statistics (DUKES) https://www.gov.uk/government/collections/digest-of-uk-energy-statistics-dukes
Rail	Annual light rail and tram statistics published by the Department for Transport https://www.gov.uk/government/collections/light-rail-and-tram-statistics London and Glasgow underground and Edinburgh tram statistics published by the Department for Transport https://www.gov.uk/government/statistical-data-sets/lrt99-london-glasgow-underground-train-statistics
Roads	Annual DfT road traffic statistics https://www.gov.uk/government/collections/road-traffic-statistics[10]

Table 8 Statistics sources for each mode

[10] Hyperlinks correct as of 3rd December 2018

Annex E: Transport incident notification thresholds

A notifiable incident is one that has an adverse effect on the security of network and information systems and that causes a significant impact on the continuity of the essential service the OES provides that meets one or more of these thresholds.

E.1 Aviation thresholds

Definition of entities in scope	Incident notification thresholds
Any entity which is granted a licence by the Secretary of State or the Civil Aviation Authority to provide en-route air traffic services in the United Kingdom.	A single incident which results in more than 10,000 unscheduled, en-route delay minutes in a 24 hour period.
Owner or manager of any aerodrome with annual terminal passenger numbers greater than 10 million. An air traffic service provider at any airport which has annual terminal passenger numbers greater than 10 million. "aerodrome" has the same meaning as in the Civil Aviation Act 1982.	Category One (more than 350,000 air transport movements annually): • A single incident which results in more than 20% of scheduled flights being cancelled in a 24 hour period.
	Category Two (150,000 to 350,000 air transport movements annually): • A single incident which results in more than 30% of scheduled flights being cancelled in a 24 hour period.
	Category Three (less than 150,000 air transport movements annually): • A single incident which results in more than 40% of scheduled flights being cancelled in a 24 hour period.
An air carrier which has: a) more than 30% of the annual terminal passengers at any UK airport which has annual terminal passenger numbers greater than 10 million; and b) more than 10 million total annual terminal passengers across all UK airports. "air carrier" has the same meaning as in Article 3(4) of Regulation (EC) No 300/2008.	(a) A single incident which results in more than 40% of the air carrier's scheduled flights from one of the airports which are in scope being cancelled in a 24 hour period; (b) A single incident which results in more than 30% of the air carrier's flights across all UK airports being cancelled in a 24 hour period; or (c) A single incident which results in any of the aerodrome thresholds being met.

Table 9 Aviation thresholds

E.2 Maritime thresholds

Definition of entities in scope	Incident notification thresholds
A shipping company which handles- (a) over 5 million tonnes of total annual freight at UK ports; and (b) over 30% of the freight at any individual UK port which fulfils at least one of the following criteria – (I) it handles more than 15% of UK total roll-on roll-off traffic; (II) it handles more than 15% of UK total lift-on lift-off traffic; (iii) it handles more than 10% of UK total liquid bulk traffic; or (iv) it handles more than 20% of UK biomass fuel traffic; or A shipping company with over 30% of the annual passenger numbers at any individual UK port which has annual passenger numbers greater than 10 million.	(a) A single incident which results in suspension of sailings across the Channel for a period of two hours or more; or (b) A single incident which results in 50% of scheduled sailings from a port being cancelled or delayed by 3 hours or more; or (c) A single incident which results in any of the incident thresholds for harbour authorities being met.
A harbour authority (as defined in section 313(1) of the Merchant Shipping Act 1995) which - (a) has annual passenger numbers greater than 10 million; or (b) fulfils at least one of the following criteria: (i) it handles more than 15% of UK total roll-on roll-off traffic; (ii) it handles more than 15% of UK total lift-on lift-off traffic; (iii) it handles more than 10% of UK total liquid bulk traffic; or (iv) it handles more than 20% of UK biomass fuel traffic.	The following thresholds only apply if that particular service is an essential service for the port (i.e. designation as an OES is because of that service, either by meeting the thresholds or through reserve power designation). (a) For passengers and roll-on roll-off traffic: A single incident that results in- (i) the port being closed for two hours or more; or (ii) 50% of scheduled sailings being cancelled or delayed by 3 hours or more. (b) For lift-on-lift-off traffic: A single incident which results in suspension of throughput at the port for 2 hours or more. (c) For liquid bulk traffic: A single incident which results in port closure with no sailings for a period of four hours or more. (d) For biomass fuel traffic: A single incident which results in- (i) port closure with no sailings for a period of four hours or more; or (ii) a 50% reduction in biomass throughput for a period of four hours or more.
(a) An operator of a port facility which handles passengers at a port which has annual passenger numbers greater than 10 million; or (b) An operator of a port facility at a port which fulfils at least one of the following criteria: (i) it handles more than 15% of UK total roll-on roll-off traffic;	The same incident notification thresholds apply as for harbour authorities.

(ii) it handles more than 15% of UK total lift-on lift-off traffic; (iii) it handles more than 10% of UK total liquid bulk traffic; or (iv) it handles more than 20% of UK biomass fuel traffic. and where that port facility operator handles the same type of freight for which the port fulfils one of the criteria mentioned in sub-paragraphs (i)-(iv). "Port facility" has the same meaning as in regulation 2 of the Port Security Regulations 2009 (SI 2009/2048)	
Operator of vessel traffic services at a port which- (a) has annual passenger numbers greater than 10 million; or (b) fulfils at least one of the following criteria: (i) it handles more than 15% of UK total roll-on roll-off traffic; (ii) it handles more than 15% of UK total lift-on lift-off traffic; (iii) it handles more than 10% of UK total liquid bulk; or (iv) it handles more than 20% of UK biomass fuel. "vessel traffic services" has the same meaning as in regulation 2(1) of the Merchant Shipping (Vessel Traffic Monitoring and Reporting Requirements) Regulations 2004 (SI 2004/2110)	A single incident which results in: (a) loss/disruption of a VTS system that causes delays in excess of two hours for 20% of ship movements within a 24 hour period; (b) the port being closed for two hours or more; or (c) any of the incident thresholds for harbour authorities being met.

Table 10 Maritime thresholds

E.3 Rail thresholds

Definition of entities in scope	Incident notification thresholds
Any operator of a mainline railway asset but excluding operators of: i. railway assets solely for the provision of international rail services; ii. railway assets for metro, tram and other light rail (including underground) systems; iii. heritage, museum or tourist railways, whether or not they are operating solely on their own network iv. networks which are privately owned and exist solely for use by the infrastructure owner for its own freight operations or other passenger or freight services for third parties and operators of passenger or freight services on those networks (including high speed rail services). "Operator" has the same meaning as in section 6 of the Railways Act 1993.	Any of the following impact thresholds are exceeded: (a) For train operators operating more than 500 trains per day: A single incident which results in 20% of a train operator's services being cancelled in a 24-hour period or in an amended timetable being run that is equivalent to that number of cancellations; (b) For train operators operating 50–500 trains per day: A single incident which results in 30% of a train operator's services being cancelled in a 24-hour period or in an amended timetable being run that is equivalent to that number of cancellations; (c) For train operators operating less than 50 trains per day: A single incident which results in 100% of a train operator's services being

"Mainline railway" means all railways in Great Britain. "Railway asset" has the same meaning as in section 6 of the Railways Act 1993. "International rail service" means a rail service where the train crosses the border of the UK and a Member State (an international border) and where the principal purpose of the service is to carry passengers or goods between stations located in the UK and stations in at least one Member State. The train may be joined and/or split, and the different sections may have different origins and destinations, provided that all carriages cross at least one international border.	cancelled in a 24-hour period or in an amended timetable being run that is equivalent to that number of cancellations; (d) A single incident that results in 5% of services cancelled nationally over a 24-hour period or an amended timetable is run that is equivalent to that number of cancellations; or (e) A single incident which results in more than 20,000 delay minutes over a period of one week or in an amended timetable being run that is equivalent to that number of delay minutes.
Operator of a railway asset for high speed rail services. "operator" and "railway asset" have the same meaning as in section 6 of the Railways Act 1993.	The same incident notification thresholds apply as with operators of rail assets for mainline and international rail services.
Operator of a railway asset for metros, trams and other light rail (including underground) systems with more than 50 million annual passenger journeys. "operator' and "railway assets" have the same meaning as in section 6 of the Railways Act 1993.	(a) For train operators operating an average of 2,500 or more scheduled services per day over a 7 day period: A single incident which results in a 2% loss of service across the network in a 24-hour period (03.00 hours to 02.59 hours); or (b) For train operators operating an average of 2,499 or less scheduled services per day over a 7 day period: A single incident which results in a 10% loss of service across the network in a 24-hour period;
Any operator of a Channel Tunnel Train (as defined in the Channel Tunnel Security Order 1994). The infrastructure manager of the Channel Fixed Link (as defined in the Channel Tunnel Act 1987). "operator" has the same meaning as in section 6 of the Railways Act 1993. "International rail service" means a rail service where the train crosses the border of the UK and a Member State (an international border) and where the principal purpose of the service is to carry passengers or goods between stations located in the UK and stations in at least one Member State. The train may be joined and/or split, and the different sections may have different origins and destinations, provided that all carriages cross at least one international border.	(a) A single incident which results in the tunnel operating below full capacity for a period of 2 hours or more; (b) A single incident which results in services being suspended for one or more operators for 2 hours or more; (c) A single incident which results in 30% of a train operator's scheduled high speed services being cancelled in a 24-hour period or in an amended timetable being run that is equivalent to that number of cancellations; or (d) For rail freight operators: A single incident resulting in 100% of a train operators services being cancelled in a 24-hour period or in an amended timetable being run that is equivalent to that number of cancellations.

Table 11 Rail thresholds

E.4 Roads thresholds

Definition of entities in scope	Incident notification thresholds
A road authority responsible for roads in the United Kingdom that annually in total have vehicles travelling more than 50 billion miles on them. A road authority that provides an Intelligent Transport Systems service that covers roads in the United Kingdom that annually in total have vehicles travelling more than 50 billion miles on them. "road authority" has the same meaning as in Article 2(12) of Commission Delegated Regulation (EU) 2015/962 "Intelligent transport system" has the same meaning as in Article 4(1) of Directive 2010/40/EU of the European Parliament and of the Council.	For roads authorities that meet the 50 billion miles threshold for designation: • A single incident that results in the flow of traffic on a road being stopped in one or both directions for a period of more than 4 hours. For roads authorities that don't meet the 50 billion miles threshold but are designated using the reserve power in regulation 8(3): • A single incident that results in serious and/or severe congestion within an area for a period of 6 hours or more.

Table 12 Roads thresholds

Annex F: Incident notification template

This form is intended to be used by Operators of Essential Services (OES) to capture initial information on NIS incidents which should be sent to the DfT Cyber Compliance Team. This form can also be used by OES to report cyber incidents to DfT and the NCSC on a voluntary basis.

Notifications must be made **as soon as possible and in any event no later than 72 hours after the OES is aware that a notifiable incident has occurred.**

For voluntary cyber incident reporting, it should be sent via email to the NCSC, and where appropriate, other contacts as set out in guidance.

Points to capture	Response
Name of person reporting Role in the company Phone Email	
Name of the Organisation and the essential service it provides Internal incident ID number or name	
Date and time incident detected Date and time incident reported	
Type of incident Cyber / non-cyber / both	
Incident status Detected incident / suspected incident	
Incident stage Ongoing / ended / ongoing but managed	
Cyber incidents – Please provide a summary of your understanding of the incident, including any impact to services and/or users, including: • Incident type • Description of the incident • How the incident was discovered • Duration • Location of the incident(s) • Services/systems affected • Impact on those services/systems • Impact on safety to staff or public • Suspected cause • Whether there is any known or likely cross-border impact • Any other relevant information	

What investigations and/or mitigations have you or a third party performed or plan to perform
Who else has been informed about this incident? (CSIRT, NCSC, NCA, other Member States etc.)
What are your planned next steps?

Table 13 Incident notification template