NIS | Competent Authority

Department of Finance
NIS Competent Authority
Enforcement Guidance

Contents

Introduction and Purpose 3
Enforcement Objectives 3
Duties and Requirement of Operators of Essential Service 4
Competent Authority Enforcement Powers 5
NIS CA Enforcement Framework 5
Enforcement Principles 5
Enforcement Action – General Considerations 6
DoF Enforcement Approach 6
Enforcement Stages 7
- Information Gathering 7
- Investigation 7
- Enforcement Determination 8
- Enforcement Action 8
- Opportunity for Appeal 8
- Decision of the First-tier Tribunal 10

Enforcement Instruments explained 11
- Information Notices 11
- Powers of Inspection 11
- Enforcement Notices 13
- Penalties 14
- Penalty Determination 16
- Material Contravention 16

Recovery of Penalties 17
Appeals 17
Publication of Enforcement Action 18
Appendix A – NIS Enforcement process 19

Introduction and Purpose

The Department of Finance (DoF) is the designated under the Network and Information Systems (NIS) legislation 2018 as the Competent Authority within Northern Ireland for Operators of Essential Service (OES) in the energy, transport (road and rail) health and drinking water supply and distribution sectors. The DoF as the Competent Authority has two main functions; (i) compliance & enforcement, and (ii) new policy and legislation.

- The Compliance & Enforcement team are responsible for oversight and implementing the NIS regulatory function, issuing guidance and assessment of operators of essential services against the NIS regulations and where necessary undertaking enforcement activities.
- The Policy & Legislation unit is responsible for evaluating the implications of new Westminster legislation and providing relevant information to the Department for Science, Innovation and Technology as the UK Department leading on this work; and ensuring appropriate application of the NIS Regulations 2018.

This guidance is developed by the Department of Finance pursuant to, and in satisfaction of, Regulation 3(3)(b) and the Competent Authority obligation to prepare and publish guidance.

The Network and Information Systems Regulations 2018 set out duties for competent authorities, operators of essential service and digital service providers, and other bodies. The Regulations also set out enforcement powers that competent authorities may use to enable them to regulate in an effective, reasonable and proportionate way.

This document provides information on the Department's enforcement powers and gives transparency on the framework and enforcement process to enact these powers on finding evidence of contravention to the NIS Legislation 2018 duties set out to the Operator of Essential Service.

This document is only for Operators of Essential Service regulated by the Department of Finance. Other Operators of Essential Service or relevant digital service providers (RDSP) should seek guidance from their respective Competent Authority.

The document sets out the general intent and principles underpinning the Department's approach to enforcement and how, and in what circumstances, the Department will exercise enforcement powers.

Enforcement Objectives

The objective of the Department of Finance's enforcement work is to protect the delivery of essential services and to ensure that operators of essential services comply with their obligations under the NIS regulations. However, enforcement action may be necessary to ensure that operators comply with the regulations and to protect the services they offer. It is ultimately the responsibility of businesses to be aware of, and comply with, the law.

The Competent Authority believes that in most cases, working with those it regulates, in a positive and practical manner through its "prevention rather than cure" approach will achieve compliance with the legislation. However, where there are breaches of the legislation we will take appropriate enforcement action.

The significance and impact of breaches will vary considerably. Assessment of priority and conduct of actions will be guided by the key principles of enforcement below.

In addition to taking enforcement action, as part of the Department's wider objectives we will also consider:

- engagement to encourage preventative action to protect essential services;
- remedial action to repair any damage;
- how ongoing compliance can be assured;
- deterrence to prevent further breaches of the law.

Duties and Requirement of Operators of Essential Service

The NIS Regulation sets out duties for Operators of Essential Service related to the security of their network and information systems - regulation 10 and the requirement to report incidents to the relevant Competent Authority - regulation 11(1). The regulations place a number of other requirements on operators that includes the following:

- Regulation 8(2) - Where an organisation meets a threshold requirement set out in Schedule 2 of the regulations, it must notify the relevant Competent Authority about this, within three months. This is effectively notification to the Competent Authority that the organisation is an Operator of Essential Service under the regulations although the organisation is, defacto, an operator in any event;
- Regulation 8A – An operator whose head office is outside the UK must nominate a responsible person and keep this information, including contact details, up-to-date;
- Regulation 10(1) – Operators must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of their network and information systems;
- Regulation 10(2) – Operators must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of their network and information systems;
- Regulation 11(1) – Operators must notify the Competent Authority about serious incidents within 72 hours;
- Regulation 11(3) – Operators must supply the Competent Authority with particular information about incident reported under regulation 11(1);
- Regulation 12(9) – Operators must notify the Competent Authority about any RDSP incident affecting the operator's essential service;
- Regulation 15 – Operators must comply with information notices served by the relevant competent authority;
- Regulation 16(1)(c) – Operators must comply with the Competent Authority's direction to appoint an inspector to conduct an inspection on its behalf; and
- Regulation 16(3) – Operators must comply with stipulations around inspections.

The regulations also require operators to take other considerations into account when completing their statutory duties. For example, operators must:

- under regulation 10(3), have regard to the state of the art to ensure a level of security of network and information systems appropriate to the risk posed in relation to their security duties;

- under regulation 10(4), have regard to any relevant guidance issued by the Competent Authority when carrying out their security duties; and
- under regulation 11(12), have regard to any relevant guidance issued by the Competent Authority when carrying out their incident-reporting duties.

Competent Authority Enforcement Powers

The NIS Regulations 2018 provides powers of enforcement that can be used by the NIS Competent Authority. Where the Competent Authority has reasonable grounds to believe that an operator has failed to comply with the NIS Regulations 2018 it can use a number of enforcement measures which include:-

- Information Notices;
- Powers of Inspection;
- Enforcement Notices; and
- Financial Penalties.

NIS CA Enforcement Framework

The Competent Authority NIS enforcement framework covers the end-to-end process through which the Competent Authority will regulate operators and take action where breaches occur.

The framework is based on a fundamental principle that adherence to the legislation should be achieved through co-operation, collaboration and consensus where possible; but enforcement action will be taken when necessary. The Competent Authority will draw on the enforcement instruments deemed most applicable for the enforcement stage or severity of the breach.

The framework sets out underpinning principles, considerations and a number of steps that may be taken by the Competent Authority to ensure compliance with the regulations.

Enforcement Principles

The Department's approach to investigating any potential contravention and making enforcement related decisions will be rigorous, thorough, evidence-based and fair, to ensure that the outcomes reached are proportionate, appropriate, reasonable and consistent.

The Department's approach to enforcement will include assessing and, where necessary, investigating, any NIS contravention and deciding what enforcement action, if any, is needed having regard to:

- the Legislation;
- Regulatory Reform Act 2006;
- the Regulators' Code;
- "Better Regulation - An Action Plan for Reform, March 2016" and its principles of:
    - Proportionality;
    - accountability;
    - consistency;
    - transparency;
    - targeting;

  - collaboration;
  - support;
  - regard for economic growth; and
- Growth Duty.

Enforcement Action – General Considerations

In compliance with regulation 23(1) before embarking on enforcement action under regulation 7(1) or (2), or A20, the Competent Authority will consider whether it is reasonable and proportionate, on the facts and circumstances of the case, to take action in relation to the contravention.

In compliance with 23(2) we will have regard to the following matters:

a) any representations made by the OES about the contravention and the reasons for it, if any;
b) any steps taken by the OES to comply with the requirements set out in these Regulations;
c) any steps taken by the OES to rectify the contravention;
d) whether the OES had sufficient time to comply with the requirements set out in these Regulations; and
e) whether the contravention is also liable to enforcement under another enactment.

Any enforcement notices or documents will be served in accordance with regulation (24) and to an appropriate person (as defined in regulation 24(2-5)). The primary method of communication will be electronically in accordance with 24(1)(c).

DoF Enforcement Approach

The Competent Authority's preferred approach to NIS regulation and administration is "prevention rather than cure." While we prefer to work collaboratively with OES to ensure compliance it is the legal responsibility of an OES to comply with the regulations and take appropriate and proportionate action to do so. Failure to do so, will result in the Competent Authority, taking enforcement action.

Any action will be in line with the regulations and pursuant to Regulation 23 and the general considerations will be taken into account.

The Competent Authority can instigate an enforcement instrument as deemed appropriate. A stepped approach of informal and formal regulatory action to enforcement will be adopted leading to financial penalties of up to £17M and remediation activity to redress compliance concerns set out by the Competent Authority.

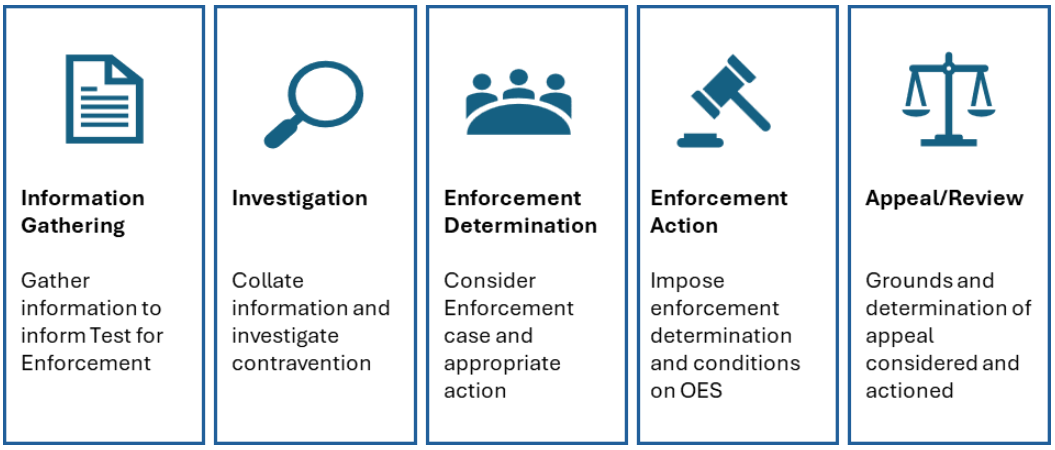
The Competent Authority will conduct an ENFORCEMENT TEST when considering whether to commence an enforcement, or to continue with a case, or whether a case can be resolved by means of engagement, inspection or an alternative resolution. The prioritisation principles below are non-exhaustive, and we may consider other factors where relevant, taking account of the facts of the case and the applicable legal framework:

a) the resources required to carry out the investigation and the availability of such resources;
b) the likely impact of the investigation in terms of the direct and indirect benefit that the investigation may bring in securing the essential service, reducing the likely impact to the service and/or impact to the consumers of the essential service and wider society and the economy;

c) the significance including the seriousness of the contravention, and the level, or likely level, of impact to consumers of the essential service or wider society and the economy;
d) the duration of the contravention;
e) whether other options are available that would be more appropriate to achieve the same or a better outcome;
f) whether taking enforcement action could deter contraventions in the future, including whether the case will have a more general deterrent effect; and
g) whether the Competent Authority is the most appropriate body to carry out a formal investigation or whether another body is better placed, is already carrying out or has already carried out such an investigation.

Enforcement Stages

In each individual case before proceeding to enforcement action, we will consider whether it is the appropriate course of action to take as set out below.



Information Gathering

This enforcement stage aligns with the “prevention rather than cure” approach and focuses on regular engagement and exchange of information, timely notification of any concerns and the opportunity to discuss and review any action requests. The Competent Authority aims, through positive collaborative discourse, to incentivise and persuade operators to take appropriate action and modify approaches, with the focus on compliance with statutory obligations and a desire to secure the network and information systems on which essential services rely. Engagement combined with assessments and audits provide the framework to assess and improve the overall security posture to the essential service and its compliance with the NIS Regulations and in a timely manner.

Investigation

While we aim for a positive, collaborative engagement there may be occasions where some information needed by the Competent Authority is not forthcoming or further investigation is needed to better understand the OES position. The Competent Authority may use information notices to enhance its understanding on the OES compliance position.

Where normal engagement and information gathering activities do not provide the Competent Authority with enough information to determine compliance with the legislation the department will open an investigation case that effectively commences a formal enforcement process.

The Competent Authority may also use the power of Inspection[1] to obtain additional information that appropriate and proportionate technical and organisational measures are being taken to manage risk.

Under regulation 16(3)(a) the Department will expect all reasonable costs for these inspections, assessments or audits will be paid by the OES within 30 days of receipt of an invoice in line with regulation 21(2).

Completion of the investigation stage the Competent Authority will consider what additional action, if any is required. If a breach of the regulation is identified this may lead to additional enforcement action being considered.

Enforcement Determination

If the Competent Authority determines that enforcement action is necessary, then an enforcement case will be established, and representation will be invited from the OES to respond to the initial findings of the Competent Authority.

The Competent Authority will consider all the evidence and representations at this stage and determine if enforcement notices and/or penalties are appropriate.

Once a determination is made, an intention to commence enforcement action will be issued to an OES outlining the type of enforcement action i.e. an intention to issue an Enforcement Notices and/or Penalty Notice and imparting our concerns and likely next steps and offering a timebound opportunity to engage with the Competent Authority and provide representation.

Enforcement Action

Where enforcement action is still deemed necessary by the Competent Authority to be appropriate, an Enforcement Action Notice will be issued to the OES.

This will be in the form of an Enforcement Notice setting out the reasons for the action and other information as set out under the Enforcement Notices section of the guidance. An Enforcement Notice may be accompanied at that time, or later, with a Penalty Notice.

Opportunity for Appeal

While every reasonable effort will be made for an OES to provide representation to the NIS Competent Authority before an instrument of enforcement is issued an OES can appeal a designation or penalty decision taken by the Competent Authority and may appeal to the General Regulatory Chamber (GRC) as the First Tier Tribunal on the grounds set out in regulation 19A(1) around designation or revocation of an OES or the serving of an Enforcement or Penalty notice.

The appeal process is governed by the General Regulatory Chamber tribunal procedure rules, "the GRC rules".

[1] Inspection can be taken to mean any form of investigation and to include activities such as assessments, inspections, tests and audits.

The GRC rules set out the procedural rules for proceedings before the General Regulatory Council as the First-tier Tribunal for the NIS Regulations 2018, including by when and how an OES should appeal and how hearings are conducted.

An OES may submit a notice of appeal within 28 days of the date on which the relevant decision or enforcement notice was received. If an OES misses the 28-day deadline, they may submit reasoning for missing the deadline to the GRC. The GRC will make the final decision to hear such an appeal after considering the information provided by the OES.

Under 19A(1) an OES may appeal to the First-tier Tribunal against one or more of the following decisions of the Competent Authority for the OES.

a) a decision under regulation 8(3) to designate that person as an OES;
b) a decision under regulation 9(1) or (2) to revoke the designation of that OES;
c) a decision under regulation 17(1) to serve an enforcement notice on that OES;
d) a decision under regulation 18(3A) to serve a penalty notice on that OES.

Under 19A(3) the OES can appeal against the decision on one or more of the grounds specified in paragraphs 19A(1) below:-

a) that the decision was based on a material error as to the facts;
b) that any of the procedural requirements under these Regulations in relation to the decision have not been complied with and the interests of the OES or RDSP have been substantially prejudiced by the non-compliance;
c) that the decision was wrong in law;
d) that there was some other material irrationality, including unreasonableness or lack of proportionality, which has substantially prejudiced the interests of the OES.

The First-tier Tribunal may, until it has determined the appeal, and unless the appeal is withdrawn, suspend the effects of the whole or part of any of the decision which the OES is appealing.

If an Enforcement Notice is not suspended in whole or part by the GRC, then it (or relevant parts of it) remain in force and can be enforced.

After considering the OES's appeal, the GRC may confirm any decision to which the appeal relates or quash the whole or part of a decision to which the appeal relates. Where the Tribunal quashes the whole or part of a decision, it will remit the matter back to the Competent Authority with a direction to reconsider the matter and make a new decision having regard to the ruling of the GRC.

The Competent Authority will reconsider the matter having regard to the direction of the GRC. If the Competent Authority makes a new decision, this will be considered final.

It should be noted that where an operator has appealed to the First-tier Tribunal under regulation 19A and the Tribunal has granted a suspension of the effect of the whole or part of the relevant decision under regulation 19B(2), the Competent Authority may not bring or continue these proceedings for as long as the suspension has effect.

Where the Competent Authority has reasonable grounds to believe that an operator has failed to comply with the requirements of an enforcement notice, the Competent Authority may seek to have

the enforcement notice applied to through civil proceedings in accordance with regulation A20 even where the operator has appealed the decision to issue the enforcement order to the First-tier Tribunal.

The Competent Authority may not commence civil proceedings before the end of a period of 28 days beginning with the day on which the last relevant enforcement notice was served on the operator.

Decision of the First-tier Tribunal

The GRC will determine the appeal in accordance with regulations after considering the grounds of appeal against 19A(3) of the NIS regulations and by applying the same principles as would be applied by a court on an application for judicial review.

The Tribunal may, until it has determined the appeal in accordance with paragraph 19B(1) and unless the appeal is withdrawn, suspend the effect of the whole or part of any of the following decisions to which the appeal relates and may as per 19B.(3):-

a) confirm any decision to which the appeal relates; or
b) quash the whole or part of any decision to which the appeal relates.

Where the Tribunal quashes the whole or part of a decision to which the appeal relates, it must remit the matter back to the designated Competent Authority for the OES with a direction to that Authority to reconsider the matter and make a new decision having regard to the ruling of the Tribunal who, must have regard to the direction given.

Where the relevant Competent Authority makes a new decision in accordance with a direction under given by the Tribunal that decision is to be considered final.

Enforcement Instruments explained

The Competent Authority can use these enforcement instruments individually or combined depending on the outcome of its determination of need.

Information Notices

Regulation 15(2) empowers the Competent Authority to issue an information notice to obtain information it reasonably requires for one or more of the following purposes:

a) to assess the security of the Operator of Essential Service's network and information systems;

b) to establish whether there have been any events that the Competent Authority has reasonable grounds to believe have had, or could have, an adverse effect on the security of network and information systems and the nature and impact of those events;

c) to identify any failure of the OES to comply with any duty set out in these Regulations;

d) to assess the implementation of the OES's security policies, including from the results of any inspection conducted under regulation 16 and any underlying evidence in relation to such an inspection.

Under 15(1) an Information Notice may also be served on any organisation to enable the Competent Authority to gather all such information that it reasonably requires to establish if the organisation is, or should be, designated as an Operator of Essential Service.

An OES must comply with the requirements of the Information Notice (15(5)) and the Competent Authority can choose to withdraw an Information Notice (15(7)).

As set out in 15(5) we will provide in writing or electronically an Information Notice which will:

- describe the information that is required;
- the reasons for requesting such information; and,
- specify the form and manner in which the requested information is to be provided; and,
- the time period within which the information must be provided.

Powers of Inspection

Under regulation 16(1)(a), the Competent Authority may carry out inspections to verify compliance with the requirements of the NIS Regulations; or in assessing or gathering evidence of potential or alleged failures to comply with the requirements of these NIS Regulations, including any necessary follow-up activity for either purpose.

The Competent Authority may also, under regulation 16(1)(b), appoint an inspector; and, under regulation 16(1)(c), direct an operator to appoint an inspector approved by the Competent Authority, to conduct an inspection on its behalf or 16(4) on such terms and in such a manner as it considers appropriate.

Regulation 16(3) set obligation of the OES to:

a) pay the reasonable costs of the inspection if so, required by the relevant Competent Authority;
b) co-operate with the inspector;
c) provide the inspector with access to their premises in accordance with paragraph 15(5)(a);
d) allow the inspector to examine, print, copy or remove any document or information, and examine or remove any material or equipment, in accordance with paragraph 15(5)(d);
e) allow the inspector access to any person from whom the inspector seeks relevant information for the purposes of the inspection;
f) not intentionally obstruct an inspector performing their functions under these Regulations; and
g) comply with any request made by, or requirement of, an inspector performing their functions under these Regulations.

Regulation 16(5) sets out duties on an inspector who may:

a) at any reasonable time enter the premises of an OES or RDSP (except any premises used wholly or mainly as a private dwelling) if the inspector has reasonable grounds to believe that entry to those premises may be necessary or helpful for the purpose of the inspection;
b) require an OES or RDSP to leave undisturbed and not to dispose of, render inaccessible or alter in any way any material, document, information, in whatever form and wherever it is held (including where it is held remotely), or equipment which is, or which the inspector considers to be, relevant for such period as is, or as the inspector considers to be, necessary for the purposes of the inspection;
c) require an OES to produce and provide the inspector with access, for the purposes of the inspection, to any such material, document, information or equipment which is, or which the inspector considers to be, relevant to the inspection, either immediately or within such period as the inspector may specify;
d) examine, print, copy or remove any document or information, and examine or remove any material or equipment (including for the purposes of printing or copying any document or information) which is, or which the inspector considers to be, relevant for such period as is, or as the inspector considers to be, necessary for the purposes of the inspection;
e) take a statement or statements from any person;
f) conduct, or direct the OES or RDSP to conduct, tests;
g) take any other action that the inspector considers appropriate and reasonably required for the purposes of the inspection.

16(6) The inspector must:

a) produce proof of the inspector's identity if requested by any person present at the premises; and
b) take appropriate and proportionate measures to ensure that any material, document, information or equipment removed in accordance with paragraph (5)(d) is kept secure from unauthorised access, interference and physical damage.

16(7) Before exercising any power under paragraph 16(5)(b) to (d) or (g), the inspector:

a) must take such measures as appear to the inspector appropriate and proportionate to ensure that the ability of the OES to comply with any duty set out in these NIS Regulations will not be affected; and
b) may consult such persons as appear to the inspector appropriate for the purpose of ascertaining the risks, if any, there may be in doing anything which the inspector proposes to do under that power.

16(8) Where under paragraph 16(5)(d) an inspector removes any document, material or equipment, the inspector must provide, to the extent practicable, a notice giving:

a) sufficient particulars of that document, material or equipment for it to be identifiable; and
b) details of any procedures in relation to the handling or return of the document, material or equipment.

Enforcement Notices

In compliance with 17(2A) before serving an enforcement notice, we will inform the operator about:

a) the alleged failure; and
b) how and by when representations may be made in relation to the alleged failure and any related matters.

Having provided the information in 17(2A) we may also provide a notice of intention to serve an enforcement notice(17(2B)).

After having regard to any representations being made by the OES and the facts and circumstances of the case, we may serve an enforcement notice on the OES within a reasonable time, irrespective of whether we have provided any notice of an intention to serve an enforcement notice has been provided.

Where an enforcement notice is served in compliance with 17(3), the Competent Authority will set out in writing:

a) the reasons for serving the notice;
b) the alleged failure which is the subject of the notice; and
c) what steps, if any, must be taken to rectify the alleged failure and the time period during which such steps must be taken

The Competent Authority may issue an enforcement notice in compliance with regulation 17(1) where there is reasonable grounds to believe than an operator has not fulfilled the requirements of the legislation. The Competent Authority may issue an enforcement notice as follows:

- Regulation 17(1)(za) – where an operator fails to notify a Competent Authority that it meets a threshold requirement, within three months of this being the case, as required under regulation 8(2);

- Regulation 17(1)(zb) – where an operator fails to nominate a responsible person where the organisation's head office is outside the UK or keep these details up-to-date, as required by regulation 8(3);
- Regulation 17(1)(a) – where an operator fails to fulfil its security duties under regulation 10(1) and (2);
- Regulation 17(1)(b) – where are operator fails to notify a Competent Authority about an incident as required under regulation 11(1);
- Regulation 17(1)(c) – where an operator fails to provide relevant detail about an incident as to the Competent Authority as required under regulation 11(3);
- Regulation 17(1)(d) – where an operator fails to notify a Competent Authority about an RDSP incident that affected its essential service;
- Regulation 17(1)(e) – where an operator fails to comply with an information notice served by the Competent Authority;
- Regulation 17(1)(f)(i) – where an operator fails to comply with the Competent Authority's direction to appoint an inspector to conduct an inspection on its behalf, as required by regulation 16(1)(c); and
- Regulation 17(1)(f)(ii) – where an operator fails comply with stipulations around inspections as set out in regulation 16(3)(a)–(g).

As set out in regulation 17(3A) an operator upon whom an enforcement notice has been served under paragraph (1) or (2) must comply with the requirements of the notice even if it has also paid a penalty under regulation 18 relating to the same contravention.

If the Competent Authority is satisfied that no further action is required, having considered:

(a) any representations submitted by the operator; or

(b) any steps taken to rectify the alleged failure, it must inform the operator, in writing, as soon as reasonably practicable.

The operator may request reasons for a decision to take no further action within 28 days of being informed of that decision.

On receipt of such a request, the Competent Authority must provide written reasons for its decision within a reasonable time and no later than 28 days after the request was made.

Penalties

A Competent Authority may serve a notice of intention to impose a penalty under regulation 18(1) if it has reasonable grounds to believe that an operator has failed to comply with particular elements of the legislation or if it has failed to comply with an enforcement order.

The sum of any penalty imposed under regulation 18 must be an amount that the Competent Authority determines is appropriate and proportionate to the failure in respect of which it is imposed; and is in accordance with the amounts set out in regulation 18(6). The levels of fines, and the classifications set out in regulation 18(6), are considered under the heading 'sum of penalty' below.

The operator will be given an opportunity to provide representations in relation to any penalty notice.

The Competent Authority will set out in writing:

a) the reasons for imposing a penalty;
b) the sum that is intended to be imposed as a penalty and how it is to be paid;
c) the date on which the notice of intention to impose a penalty is given;
d) the period within which a penalty will be required to be paid (the "payment period") if a penalty notice is served and the date on which the "payment period" is to commence;
e) that the payment of a penalty under a penalty notice (if any) is without prejudice to the requirements of any enforcement notice (if any); and
f) how and when representations may be made about the content of the notice of intention to impose a penalty and any related matters.
g) Details of the appeal process as set out under regulation 19A; and
h) Specify the consequences of failing to make payments within the payment period.

It is the legal duty that an operator must comply with any requirement imposed by a penalty notice under regulation 18(3E).

It is important to note that a Competent Authority may serve a notice (intention to impose a penalty or final penalty notice) whether or not it has served, or is serving, an enforcement notice on the operator – regulation 18(3C).

After consideration the Competent Authority may withdraw a penalty notice by informing the person upon whom it was served in writing. – regulation 18(4)

After considering any representations made by the operator, if the Competent Authority is satisfied that a penalty is warranted given the circumstances it may serve a notice of intention to impose a penalty notice under regulation 18(1), or a final penalty notice under regulation 18(3A) in respect of the following requirements:

- Regulation 8(2) – requirement to notify Competent Authority where organisation/operator meets a threshold requirement within three months;
- Regulation 8A – requirement to nominate a responsible person where operator's head office is outside the UK;
- Regulation 10(1) – requirement to take appropriate and proportionate technical and organisational measures to manage risks posed to the security of their network and information systems;
- Regulation 10(2) – requirement to take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of their network and information systems;
- Regulation 11(1) – requirement to notify the Competent Authority about serious incidents within 72 hours;
- Regulation 11(3) – requirement to supply the Competent Authority with particular information about incident reported under regulation 11(1);

- Regulation 12(9) – requirement to notify the Competent Authority about any RDSP incident affecting the operator's essential service;
- Regulation 15 – requirement to comply with information notices served by the relevant Competent Authority;
- Regulation 16(1)(c) – requirement to comply with a CA's direction to appoint an inspector to conduct an inspection on its behalf;
- Regulation 16(3) – requirement to comply with stipulations around inspections; and
- Regulation 17(3A) – requirement to comply with an enforcement notice.

Penalty Determination

The Competent Authority will use the following criteria when determining the level of any financial penalty:

1. assess the level of contravention or failure – material or not material;
2. assess the seriousness of the contravention or failure and place within the applicable identified penalty category;
3. consider any indirect consequence of impact on NI society or the economy;
4. consider aggravating and mitigating factors;
5. consider an adjustment for deterrence;
6. Determine % of turnover (growth duty) and economic impact; and
7. establish the total financial amount.

Where enforcement action results in a penalty being issued, the sum of any penalty imposed under the regulation will be determined by the Competent Authority, as appropriate and proportionate in relation to the failure in respect of which it is imposed. The level of penalty will be assessed across three categories:

1. Not a material contravention;
2. A material contravention but not considered to have created a significant risk to, or significant impact on, or in relation to, the service provision provided by the operator; and
3. A material contravention that the Competent Authority determines has or could have created a significant risk to, or significant impact on, or in relation to, the service provision by the operator.

For each of the three contravention categories, the penalty limits are:

- Category 1 - the amount must not exceed £1,000,000.
- Category 2 - the amount must not exceed £8,500,000.
- Category 3 - the amount must not exceed £17,000,000.

Material Contravention

For the purposes of informing the extent of a Penalty under regulation 18 it is necessary to understand the level of impact or materiality. A Material contravention means: a failure to take, or adequately take, one or more of the steps required under an enforcement notice within the period specified to rectify a failure described in one or more of sub-paragraphs of regulation 17(1)(a) to (d).

A material contravention also covers a failure, even if no enforcement notice was served. Therefore, a breach of one of the following requirements may be classified as a material contravention for the purposes of regulation 18:

- Regulation 17(1)(a) – an operator fails to fulfil its security duties under regulation 10(1) and (2);
- Regulation 17(1)(b) – an operator fails to notify a Competent Authority about an incident as required under regulation 11(1);
- Regulation 17(1)(c) – an operator fails to provide relevant detail about an incident as to the Competent Authority as required under regulation 11(3); and
- Regulation 17(1)(d) – an operator fails to notify a Competent Authority about an RDSP incident that affected its essential service.

The Competent Authority must consider whether the material contravention created a significant risk to, significant impact on, or in relation to, the service provision provided by the OES. However, it should also be noted that the level of any fine will take into account the facts and circumstances of the case.

For the purposes of regulation 18, a breach of the following requirements would not be considered a material contravention and might attract a fine up to £1,000,000:

- failure to notify the Competent Authority under regulations 8(2);
- failure to comply with the requirements stipulated in regulations 8A relating to nomination by an OES of a person to act on its behalf in the UK;
- failure to comply with an information notice issued under regulation 15;
- failure to comply with a direction given under regulation 16(1)(c) in relation to an inspection;
- failure to comply with the requirements stipulated in regulation 16(3) relating to inspections.
- Failure to comply with regulation 17(3A) where an enforcement notice has been served under paragraph 17(1), designation of an OES, he OES must comply with the requirements, if any, of the notice regardless of whether the OES has paid any penalty imposed on it under regulation 18.

Recovery of Penalties

Where a Penalty Notice has been served under regulation 20(4), a penalty is recoverable as if it were payable under an order of a county court or of the High Court. In accordance with regulation 20(5), a penalty will be taken forward under Article 116 of the Judgments Enforcement (Northern Ireland) Order 1981 (register of judgments) as if it were a judgment in respect of which an application has been accepted under Article 22 or 23(1) of that Order.

Appeals

While every reasonable effort will be made for an OES to provide representation to the NIS Competent Authority before an instrument of enforcement is issued an OES can appeal a designation or penalty decision taken by the Competent Authority and may appeal to the General Regulatory Chamber (GRC). The appeal process is governed by the General Regulatory Chamber tribunal

procedure rules, "the GRC rules" and an OES may submit a notice of appeal within 28 days of the date on which the relevant decision or enforcement notice was received. More information on Appeals is outlined in the Opportunity for AppealEnforcement Stages Opportunity for Appeal section.

Publication of Enforcement Action

Given the sensitivities around the NIS sectors and risk to critical national infrastructure it would not be DoF Policy to publish findings or enforcement action which may highlight inherent vulnerabilities or weaknesses within an OES. However, if deemed in the public or wider NIS community interest DoF reserve the right to publish outcomes of enforcement action.

Appendix A – NIS Enforcement process