Department for
Digital, Culture
Media & Sport

Security of Network and Information Systems

Government response to public consultation

January 2018
Department for Digital, Culture, Media and Sport

CONTENTS

1. Contact details

This document is the Government's response to the public consultation, *Security of Network and Information Systems Public Consultation of August 2017*. It will cover:

- a detailed response to the questions raised in the consultation

Comments on the Government's response can be sent to:

NIS Directive Team
Department for Digital, Culture, Media & Sport
4th Floor
100 Parliament Street
London
SW1A 2BQ

Telephone: 020 7211 6000.
Email niscallforviews@culture.gov.uk

This report is also available at www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive. Alternative format versions of this publication can be requested from the above address.

Complaints or comments If you have any complaints or comments about the consultation process you should contact the NIS Directive Team at the above address.

Freedom of Information

Information provided in the course of this consultation, including personal information, may be published or disclosed in accordance with access to information regimes, primarily the Freedom of Information Act 2000 (FOIA) and the Data Protection Act 1998 (DPA).

The Department for Digital, Culture, Media and Sport will process your personal data in accordance with the DPA and, in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties. This consultation follows the UK Government's consultation principles.

2. Executive summary

As our reliance on technology grows, improving the security and resilience of the UK's essential services is increasingly important and is an essential requirement for a prosperous UK economy. We need to secure our technology, data and networks in order to keep our businesses, citizens and public services protected. The National Cyber Security Strategy published on 1 November 2016 set our vision for the UK in 2021 as secure and resilient to cyber threats, prosperous and confident in the digital world.

On 8 August 2017, the Government published its proposals for improving the security of the UK's essential services, through its plans to implement the Security of Network and Information Systems Directive (known as the NIS Directive), in a public consultation. This consultation covered six main topics -

- How to identify essential services
- A national Framework to manage implementation
- The security requirements for operators of essential services
- The incident reporting requirements for operators of essential services
- The requirements on Digital Service Providers
- The proposed penalty regime

The Government received over 350 responses to its consultation. These responses showed that there was broad support for the Government's approach and that in the main, the Government's proposals were thought to be appropriate and proportionate. More detailed analysis of the responses to the consultation can be found in the accompanying analysis paper on the consultation web page: www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive.

Respondents also highlighted areas of concern and the Government has attempted to address these through changes to its approach. The main changes that the Government proposes to make are clarifying:

- the thresholds required to identify operators of essential services;
- the role of the Competent Authority and how powers may be delegated to agencies;
- that the role of the National Cyber Security Agency is limited to cyber security;
- the expectations on operators within the first year or so; and
- the definitions of Digital Service Providers

The Government also intends to simplify:

- the incident response regime to separate incident response procedures from incident reporting procedures; and
- the penalty regime slightly, to reduce the risk of fines in excess of £17m.

The Government believes that these changes will provide further reassurance to industry. The Government again reiterates that our approach will remain reasonable, proportionate and appropriate and that the Government and Competent Authorities will work closely with industry to ensure that this legislation will be a success.

Background on the NIS Directive

The NIS Directive was adopted by the European Parliament on 6 July 2016. Member States have until 9 May 2018 to transpose the Directive into domestic legislation. The NIS Directive provides legal measures to boost the overall level of network and information system security in 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 Single Point of Contact (SPOC), and a national NIS competent authority (or authorities);

- Setting up a Cooperation Group, to support and facilitate strategic cooperation and the exchange of information among Member States. Member States will also need to participate in a CSIRT Network to promote swift and effective operational cooperation on specific network and information system security incidents and as well as the sharing of information about risks;

- Ensuring the framework for the security of network and information systems is applied effectively across sectors which are vital for our economy and society and which rely heavily on information networks, including the energy, transport, water, healthcare and digital infrastructure sectors. Businesses in these sectors that are identified by Member States as “operators of essential services” will have to take appropriate and proportionate security measures to manage risks to their network and information systems. Operators of essential services will also be required to notify serious incidents to the relevant authority. Key digital service providers (search engines, cloud computing services and online marketplaces) will also have to comply with the security and incident notification requirements established under the Directive.

On 23 June 2016, the EU referendum took place and the people of the United Kingdom voted to leave the European Union. Until exit negotiations are concluded, the UK remains a full member of the European Union and all the rights and obligations of EU membership remain in force. During this period the Government will continue to negotiate, implement and apply EU legislation. The outcome of these negotiations will determine what arrangements apply in relation to EU legislation in future once the UK has left the EU. It is the UK Government’s intention that on exit from the European Union these policy provisions will continue to apply in the UK.

3. Essential services

The consultation responses highlighted concerns by a large proportion of respondents that the identification thresholds, used to define who is in scope of the requirements of the Directive, required greater clarity. Lead Government Departments have been refining these thresholds, so that they are clearer and so that companies can identify with certainty whether they are in scope of the Directive. Revised thresholds are attached at **Annex 1**.

When considering these thresholds, the Government has taken into account the requirements of the Directive as set out in Article 5 (Identification of Operators of Essential Services) and Article 6 (Significant Disruptive Effect). All the parameters set out in these two Articles were taken into account, although the Government focused on those that were most relevant for each sector in order to identify key operators. The thresholds set out in the consultation and this response are the result of that work.

A number of respondents questioned what systems controlled by an Operator would be in scope. The thresholds in Annex 1 are not intended to identify the systems that are in scope of the Directive (which will be the responsibility of the Operator in discussion with the Competent Authority), only the Operators of Essential Services. Identifying the systems that support the services will need to be carried out by the Operators, as part of understanding how they can comply with the security requirements.

A number of respondents called on the Government to broaden the scope of the Directive to include additional sectors, such as Government, Chemicals, Food and Agriculture, or other entities beyond those listed in the Directive. At this stage, the Government's priority is to maintain the Directive's scope in terms of the sectors and entities to which it relates and not 'gold-plate' our implementation by including additional sectors at this time. The Government intends to conduct a post-implementation review three years after the legislation comes into effect and this review will consider the effectiveness of the regulations. A decision to extend the scope of the regulation would be considered at that time.

A number of respondents asked questions about the reserve power to designate operators that do not meet the identification threshold for their sector. This reserve power is only intended to be a limited tool for use where specific operators do not meet the identification threshold (column four of the table at Annex 1), but whom the Government believes there is a compelling case that this should be within scope. The Government considers that it is essential to have a power to designate operators to ensure that essential services are protected without imposing unnecessary regulatory burdens on other organisations. In any use of this power, the Operator will still need to meet the sector, subsector and essential service requirements (columns 1 to 3 of the table at Annex 1). This power cannot be used to designate an entity who does not meet those requirements.

The Government only intends to use the reserve power where there are valid reasons on the grounds of:

- national security;

- a potential threat to public safety; or
- the possibility of significant adverse social or economic impact resulting from a disruptive incident.

4. National framework

The Government notes that there was broad support for our proposed multiple Competent Authority approach. The Government intends to maintain this approach. Work on finalising the list of Competent Authorities is ongoing, as the Government ensures that the Competent Authorities have adequate legislative powers to carry out their duties and adequate resources to carry out their functions. An updated list of proposed Competent Authorities is at **Annex 2**. The Competent Authorities listed are subject to final confirmation and the definitive list of Competent Authorities will be included in the NIS Regulations.

A number of responses called for a greater role for the National Cyber Security Centre (NCSC) in regulating the NIS Directive and in providing support to Operators and Competent Authorities. The Government notes the regard that industry have for the expertise of the NCSC and that part of the NCSC's role is to be the UK's centre of excellence on all cyber security matters. The NCSC is central to the successful implementation of NIS.

The Government is clear that there must be a clear separation of powers between the NCSC and Competent Authorities. This will allow NCSC to carry out its role in providing expert advice and incident response capability to cyber attacks. It is also a long standing Government policy that Lead Government Departments take responsibility for all risks including Cyber. Having NCSC as the regulator for NIS would be inconsistent with this and existing regulatory frameworks for broader Critical National Infrastructure security.

Under the UK's implementation of the NIS Directive the NCSC will undertake the advisory role of the Computer Security Incident Response Team (CSIRT). It will not be able to, or seek to, enforce actions on Operators or Digital Service Providers. We believe this is important to maintain the close working relationships that have been built between industry and government in dealing with cyber issues.

The NCSC will also be the Technical Authority for cyber security, publishing guidance and assessment tools for use by both the Competent Authority and Operators. The NCSC will draw up a framework setting out exactly the level of support that they will provide to Competent Authorities.

The Government accepts that there is a need for extra clarification on the role of the Competent Authority and how Competent Authorities will interact with each other and across other regimes such as GDPR. The Government aims to publish further guidance before May 2018 to assist Competent Authorities to carry out their functions.

Role of the Competent Authority

In addition, the following summary is intended to provide some additional clarity at this stage. A Competent Authority will be responsible for the monitoring and oversight of NIS implementation in its sector. A Competent Authority's powers will include the ability to:

- designate Operators of Essential Services,
- request information related to this Directive,
- direct an Operator or Digital Service Provider to undertake an action in relation to the NIS Directive,
- to audit, or require an audit, of an Operator of an Essential Service or Digital Service Provider
- to monitor the application of the Regulations,
- to prepare and publish guidance,
- to notify the public about an incident,
- To investigate the causes of an incident
- to enforce an instruction on an Operator of an Essential Service or Digital Service Provider,
- to apply a penalty on an Operator of an Essential Service or Digital Service Provider.

Please note, however, that this list is only indicative at this stage and the full range of powers will be set out in the implementing Regulations.

When considering whether to take specific action in relation to the Directive, a Competent Authority will need to ensure that its action is appropriate and proportionate, and should, where possible, take the following factors into account:

- any representations made by the notified Operator of an Essential Service or Digital Service Provider;
- any steps taken by an Operator of an Essential Service or Digital Service Provider towards complying with the requirements set out in the regulation;
- any steps taken by an Operator of an Essential Service or Digital Service Provider for remedying the consequences of any contraventions;
- whether the Operator of an Essential Service or Digital Service Provider has had adequate time to implement the requirements of the regulation; and
- whether an offence has also occurred under another UK regulation or law and the penalties that may be applied under that legislation.

In some circumstances a Competent Authority may wish to use other bodies to carry out some of its functions. The Government is exploring the legal framework through which this might happen. Where this is the case, the Competent Authority will make clear to its sector when and how they should expect to interact with other bodies.

A number of respondents raised concerns about risks of divergence of approaches between Competent Authorities in the multiple competent authority approach. The Government is seeking to reduce these risks by ensuring that there is common guidance for Competent Authorities (such as the guidance produced by the NCSC), by encouraging Competent Authorities to cooperate with one another, and where possible to have common procedures

where possible for investigations, assessing penalties etc. However, there will sometimes be a need for divergence between sectors, and Competent Authorities will have the flexibility to adapt their approach to reflect the needs of their sector.

Where an Operator falls under the jurisdiction of more than one Competent Authority, the Competent Authorities are encouraged to cooperate with each other, to ensure that they do not put an unnecessary burden on the Operator or make conflicting demands. However, they will retain responsibility for their jurisdiction and the Operator will have to engage with both Competent Authorities.

A number of responses raised concerns about the risk of infringing more than one piece of legislation at a time. This risk is unavoidable, as Operators will be required to comply with a wide range of legislation, not all of them linked or in similar fields. If an infringement occurs that breaches more than one piece of legislation, Competent Authorities will be required to have regard to this and where possible discuss the best approach with other regulators, but they will remain free to undertake their own response to any infringement, provided that it is appropriate and proportionate.

5. Security requirements for operators of essential services

Security requirements and high level principles

Given the broad level of support for the proposed approach to NIS security requirements based on outcome-based principles and supporting guidance, the Government does not intend to make any fundamental changes of approach.

In relation to the 14 Principles (See **Annex 3**), the Government recognises the need for some additional detail to assist organisations when they are taking decisions about implementing security measures. Some of this additional detail is available on the NCSC website where the supporting guidance is published, and it is expected that the initial version of the NIS Cyber Assessment Framework (CAF), planned for publication in Spring 2018, will provide further clarity. It is expected that determinations on acceptable levels of cyber security will be made by Competent Authorities through use of the CAF. The Government remains committed to an outcome-based approach to implementing the NIS Directive and, consequently, the statements of security requirements will, necessarily, always leave room for judgements to be made within the context of an organisation's risk management approach.

While the Government acknowledges the value of some established cyber security standards, it believes that there is no single existing standard that adequately covers NIS Directive security requirements for operators of essential services. However, in order to ensure some consistency in approach the 14 principles have been based around existing global standards and guidance.

It is the Government's intent that the 14 principles should be relevant to all networks and information systems supporting the delivery of essential services, including Industrial Control Systems and other circumstances in which legacy equipment continues to play a central role. The principles carry no assumptions about how the required outcomes should be achieved. It is for the OES to determine the most appropriate security measures within their organisational context in discussion with the relevant Competent Authority. This approach will be carried through to the supporting guidance to be published by the NCSC.

As a result of some of the specific responses concerning the wording of some of the individual principles, together with an internal process of review and improvement, changes have been made to the way some of the principles are stated and explained. The new version of the complete set of principles appears in Annex 3.

A number of respondents raised concerns about how NIS will apply to their supply chains. It is the Government's view that it is the Operator of Essential Service or Digital Service Provider's responsibility to ensure (through whatever levers or contractual arrangements they have) that their suppliers have in place appropriate measures. NIS will not apply directly to suppliers and Competent Authorities will not be enforcing NIS requirements on the supply chain of Operators of Essential Service or Digital Service Providers. Guidance on ensuring the security of the supply chain is included in the NCSC guidance.

The Government values the offers from responders to collaborate on the development of supporting guidance for NIS Directive security requirements. Following initial publication in January 2018 by the NCSC, there will be opportunities for those with a direct interest in the content of the guidance to provide views and comments to inform subsequent versions.

Expectations on Operators and Competent Authorities

There was a clear concern raised through the consultation regarding what would be expected of both Operators and Competent Authorities over the course of the first year and beyond, in relation to implementing the Directive.

The Government can reassure both Operators and Digital Service providers that the approach of both the Government and Competent Authorities in implementing the requirements of the Directive will be realistic and will take into account the circumstances of each sector as appropriate. Competent Authorities will be expected to engage with their sectors and keep them informed about the approach they intend to take.

Competent Authorities will take a reasonable and proportionate approach to enforcement and it is the Government's expectation that the process of improving the security of Network and Information Systems of the UK's essential services will take a number of years. Competent Authorities will seek to work collaboratively with industry and their focus for the initial phase is likely to be on developing a detailed picture of the current levels of security within their sector, possibly based on an initial self assessment, and in working with Operators to assess areas for further development. However, the Government wants to make clear that even in this first year, Competent Authorities will have the power to issue

penalties where significant compliance issues have been discovered and it is evident that organisations are not making active efforts to remedy them.

Operators will be in scope of the Directive if they meet the identification thresholds. Competent Authorities will be encouraged to write to their Operators in order to begin the process of working with Operators in order to help them assess their compliance. When assessing compliance with the Directive, Competent Authorities will take into account the amount of time that Operators have had to implement the requirements.

Operators will be given time to implement the necessary security measures. The Government can reassure Operators that the main priority of Competent Authorities for the first year will be in obtaining a clear picture of the security of network and information systems in their sectors. Operators will be expected to have begun analysing their systems and existing security measures in order to understand where further work needs to be done, and to develop plans in order to reach the appropriate levels of security requirements. The NCSC's Cyber Assessment Framework is likely to form the basis of these initial assessments of cyber security standards, both by Competent Authorities and Operators, although this will be dependent on the sector.

The guidance published by the NCSC sets out the Government's advice on how Operators can apply appropriate and proportionate technical and organisational measures in order to manage the risks posed to the security of network and information systems which they use in their operations. Where there is a need for sector specific guidance, to ensure the security of systems that may not fit into the broader guidance, Competent Authorities will work with Operators and the NCSC to develop this. Any sector specific guidance will be introduced in a reasonable and proportionate manner and Operators will be given time in order to implement any necessary measures.

In relation to non-cyber security issues, such as resilience, the Government does not propose to change or replace existing standards and legislation that cover these issues. Operators of Essential Services will be directed by their Competent Authority to existing requirements and measures.

6. Incident reporting for operators of essential services

The Government accepts that clearer guidance and actual thresholds to determine what a reportable incident is, are required if the NIS incident reporting systems is to work. Competent Authorities will calculate incident reporting thresholds for each sector and/or sub sector. It is the responsibility of the designated Competent Authority in each sector to publish the incident reporting thresholds that will apply under NIS. These will be published before May 2018.

In order to define incident thresholds, Competent Authorities must determine what a significant impact would be in their sectors. It is the Government's view that as each sector differs in terms of existing regulatory requirements, and faces different cybersecurity

challenges, determining what is a significant impact should be done on a sector-by-sector basis. Where necessary these thresholds can also be determined on a sub-sector or micro sector basis provided they are applied consistently to all operators in that sub or micro sector.

As a minimum, the following parameters will be used:

(a) the number of users affected by the disruption of the essential service;
(b) the likely or actual duration of the incident;
(c) the geographical spread (area affected by the incident);

In addition to these three parameters, Competent Authorities may also use the following optional parameters:

(d) the dependency of other sectors on the service provided by the affected entity;
(e) the impact that incidents have, in terms of degree and duration, on economic and societal activities, public safety or national security;

Whilst these additional parameters are optional per sector, if used, they should be applied to all operators within a sector, unless there are specific clear and justifiable reasons for divergence between jurisdictions.

New structure

As a result of feedback during the Consultation, the Government is amending its proposed incident reporting structure for NIS. This change is intended to separate incident response from incident notification. Incident response being considered primarily as a support function for Operators, where the Government can provide assistance, and incident reporting a more regulatory notification process.

All NIS incidents (i.e. incidents that meet the parameters set out above and published by the Competent Authority) should be reported to the Competent Authority. The Competent Authority will then log the incident and decide if any follow up investigation is required. This will be a standalone process and will not form any part of the incident response. Voluntary reporting can be reported to either the Competent Authority or NCSC and is actively encouraged.

If companies require incident response support, they should approach the NCSC for assistance on cyber related incidents (e.g. DDoS attacks, Malware, hacking etc.), and their Competent Authority or relevant Lead Government Department (depending on guidance) for non cyber or resilience incidents (e.g. hardware failure, fire, physical damage etc.).

The was broad support for the Government's proposal to apply a similar timescale of 72 hours to incident reporting as for GDPR, and the Government will maintain this approach. A number of respondents recommended that the wording of the reporting requirement be the same as well, which the Government sees merit in. The Government is therefore intending to use the wording "*without undue delay and, where feasible, no later than 72 hours after*

having become aware of an incident." Competent Authorities will have the flexibility to assess a request for incident reporting after this deadline and will be able to agree to requests if they are justified.

The Government understands that these measures will involve costs to Operators, but believes that there is a strong public and national benefit from improving the security of the UK's essential services and digital service providers.

7. Digital service providers (DSP)

Although a small majority of respondents agreed with the Government's proposal to define Digital Service Providers, it is clear that this continues to be a challenge. Defining Digital Service Providers in a manner that is both compatible with the Directive and clear to individual Digital Service Providers is not simple. The Government's intention has always been to try to make it clear who was in scope and who was without, and to limit the scope of those who have to comply with the Directive to those companies whose loss of service could have the greatest impact on the UK economy either directly or through impact on other companies.

A number of respondents requested that the definitions be amended to exclude Software as a Service. The Government believes that Software as a Service providers play an important role in the UK's economy and it is right that they are held responsible for ensuring the security of their network and information systems. It considers its approach, as revised below, is appropriate, in line with the requirements of the Directive, and will ensure that only those Software as a Service providers that provide elastic and scalable resources to their customers are included.

The regulations implementing the NIS Directive will reflect the wording of the Directive:

- "**digital service**" means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council which is a type listed in Annex 3 [of the Directive]";

- "**digital service provider**" means any legal person that provides a digital service;

- "**online marketplace**" means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;

- "**online search engine**" means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input and returns links in which information related to the requested content can be found;

- "**cloud computing service**" means a digital service that enables access to a scalable and elastic pool of shareable computing resources;

In order to assist the Competent Authority and Digital Service Providers in recognising when a DSP is in scope of this Directive the Government proposes to provide the following clarifications through Guidance:

Online marketplaces

- An online marketplace should be defined as a platform that acts as an intermediary between buyers and sellers, facilitating the sale of goods or services, i.e. a service that enables consumers and traders to conclude online sales or service contracts with traders, and it represents the final destination for the conclusion of those contracts.

- Sites that redirect users to other services to make the final contract (e.g. price comparison sites), or that only connect buyers and sellers to trade with each other (e.g. classified advert sites), or that only sell directly to consumers on behalf of themselves (e.g. online retailers), are not in scope.

Online search engines

- 'online search engine' means a digital service that allows users to perform searches of the 'public parts of the worldwide web' in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.

- Where a site offers search engine facilities as outlined above, but those facilities are powered by another search engine, then the underlying search engine is required to meet the requirements of the NIS Directive. Internal organisational search engines, that do not facilitate external searches of the internet are not in scope.

Cloud computing services

- 'cloud computing service' means any Digital Service Provider that enables access to a scalable and elastic pool of shareable physical or virtual resources.

- The Government considers that this primarily (but not exclusively) includes Digital Service Providers that provide public cloud services of the following nature:

    - "'Infrastructure as a Service' (IaaS) - the delivery of virtualised computing resource as a service across a network connection, specifically hardware – or computing infrastructure - delivered as a service;
    - 'Platform as a Service' (PaaS) - services that provide developers with environments on which they can build applications that are delivered over the internet, often through a web browser; and
    - 'Software as a Service' (SaaS), provided the resources available to the customer through that software are changeable in an elastic and scalable way. The Government considers that this would likely exclude most online gaming, entertainment or VOIP services, as the resources available to the user are not

scalable, but may include services such as email or online storage providers, where the resources are scaleable.

Since the consultation was launched, the European Commission has published a draft Implementing Act, which set out the security measures and incident reporting thresholds that DSPs will need to comply with. However, at the time of writing this response, this Implementing Act has yet to be agreed by Member States and remains only as a draft.

The Government is committed to carrying out a further targeted consultation once Implementing Act is approved by Member States. This consultation will be limited to how the UK proposes to implement and carry out the requirements of the Implementing Act as neither the UK nor any other Member State will have flexibility to amend the Implementing Act once it has been agreed.

The Government's approach is likely to be based around ensuring consistency with the Single Market, so that Digital Service Providers can have a consistent approach in regard to security standards measures across the UK and the Single Market, and is likely to follow the guidance published by the European Network and Information Systems Agency (ENISA).

The Government understands that these measures will involve costs to Digital Service Providers, but believes that there is a strong public and national benefit from improving the security of the UK's Digital Service Providers. The Government will try to minimise these costs where possible, through applying consistency in approach to EU partners and other existing compatible reporting regimes, and ensuring that Digital Service Providers only have to report to a single point.

The Government can reassure Digital Service Providers that both it, and the Competent Authority will approach implementation of the NIS Directive in a reasonable fashion. Companies will be given time to implement the requirements of the Directive.

8. Penalty regime

The Government received significant feedback on its proposed penalty regime. The Government's priority in considering an appropriate penalty regime was to improve the cyber security of UK, and considers the aim of an effective penalty regime is to provide a mechanism to enforce this. The Government believes that an appropriate penalty regime should be significant enough to incentivise a change in behaviour while remaining proportionate.

There are different considerations that apply to different sectors when considering the appropriate level of penalty - for example, what is suitable for the Health sector might not be suitable for the energy sector, and vice versa. There will be consistency in how a Competent Authority should approach fines - Competent Authorities must be reasonable, appropriate, and proportionate, take account of mitigating factors when considering penalties, and consider fines only as a last resort. However, it should also be noted that what will be considered a proportionate penalty will vary between sectors and that Competent Authorities

will have the flexibility to be able to make an assessment based on their own judgement, the evidence available, and the impact of the contravention.

The Government continues to believe that the principle of linking NIS penalties with the GDPR is right approach as the impact of an incident under NIS could have significant impact on the economy or an individual to an equal or greater extent than GDPR (significant damage to the economy or even loss of life). However, the Government also recognises and agrees with some of the counter arguments made by respondents through the consultation, such as:

- that there is a large disparity between UK's approach and that of some other Member States;
- that there is a risk that companies may disinvest, although not to the extent raised;
- that the regime as set out may impact on the willingness of companies to voluntarily report;
- That the two penalty bands are not appropriately balanced.

The Government has therefore decided to amend the proposed penalty regime as follows:

The percentage of global turnover element will be removed from the proposed regime. The Government believes that this is what is causing the most concern for industry, and agrees that this may be considered disproportionate, especially when considered against other Member State penalty regimes.

The upper limit of penalties will be maintained at £17 million. However, the two penalty bands will be merged into a single band that will cover all contraventions. The Government's expectation is that the maximum penalty levels are precisely that, and should be reserved for the most severe cases, in an appropriate and proportionate manner.

Based on this revised approach the penalty regime for the NIS regulation will be:

- a maximum financial penalty of £17m, which will cover all contraventions, such as (for example) failure to cooperate with the competent authority, failure to report a reportable incident, failure to comply with an instruction from the competent authority, failure to implement appropriate and proportionate security measures.

As stated above, the Government believes that there is a need for a significant penalty regime and that amending the penalty regime in this manner will deliver this for the UK, whilst addressing the concerns raised by industry, and reiterates its view that penalties are a last resort.

The Government understands the perceived concern over double jeopardy, in particular in relation to the General Data Protection Regime (GDPR). The Government agrees that Operators and Digital Service Providers should not be tried for the same offence twice, but notes that there may be reason for them to be penalised under different regimes for the same event because the penalties might relate to different aspects of the wrongdoing and different impacts. This will apply not just to GDPR but other sectoral and national legislation such as safety legislation or service commitments.

The Government does not believe that 'double jeopardy' can be completely removed, without undermining either the NIS Regulations or other UK legislation. However, in order to take these considerations into account, the NIS Regulations will include text which will encourage Competent Authorities to work with regulators in the event of different regimes

applying to determine what approach to take. This will not limit a Competent Authority's ability to apply the penalty it feels is appropriate to the circumstances, but will encourage it to factor in other regimes if this is appropriate. Competent Authorities will be free to decide whether to use existing regulatory enforcement regimes or the NIS enforcement regime, if existing regimes are more appropriate to the circumstances and proposed response.

In all consideration of penalties, Competent Authorities will be required to determine that the penalty be appropriate and proportionate to the contravention in respect of which it is imposed. Competent Authorities will take into account representations from the operator, steps taken to comply with the NIS Directive, actions taken to remedy any consequences, as well as other legislation that may have been breached.

Annex 1 - Table of essential services and identification thresholds

Sector	Subsector	Essential service	Identification thresholds
Drinking water supply and distribution	n/a	The supply of potable water to households.	Operators serving 200,000 or more people.
Energy	Electricity	The function of supply (the sale or resale of electricity) to consumers.	In England, Scotland and Wales: Electricity suppliers (incl. aggregators where they act as suppliers) that meet the following two criteria (both must apply): • use of smart metering infrastructure; • supply greater than 250,000 consumers. Operators of electricity generators* with a generating capacity greater or equal to 2 Gigawatts (GW), including: • Standalone transmission connected generation; • Multiple generating units with a cumulative capacity greater or equal to 2 Gigawatts (GW); *excluding nuclear electricity generation. The government does not consider the civil nuclear sector to be in scope of the NIS Directive; In Northern Ireland: Licensed suppliers who supply to greater than 8,000 customers Any generator with a generating capacity equal to or greater than 350 MW
		Electricity (SEM Operator)	The holder of a SEM operator licence under Article 8(1)(d) of the Electricity (NI) Order 1992.
		Electricity (transmission).	In England, Scotland and Wales: Network operators with the potential

			to disrupt supply to greater than 250,000 consumers. International interconnectors and Direct Current converter station with a capacity greater than or equal to 1 Gigawatts (GW). In Northern Ireland: The holder of a transmission licence under Article 8(1)(b) of the Electricity (NI) Order 1992.
		Electricity (distribution)	In England, Scotland and Wales: Network operators with the potential to disrupt supply to greater than 250,000 consumers. In Northern Ireland: The holder of a distribution licence under Article 8(1)(bb) of the Electricity (NI) Order 1992.
	Oil	Oil transmission (upstream).	Operators with throughput of more than 20 million barrels of oil equivalent (boe) per year.
		Oil transmission (downstream). The distribution of petroleum-based fuels to other storage sites throughout the UK by road, pipeline, rail or ship.	In England, Scotland and Wales: Operators which provide or handle 500,000 tonnes of fuel per year. In Northern Ireland: Operators which provide or handle 50,000 tonnes of fuel per year.
		Oil production, refining and treatment and storage (upstream).	Operators with throughput of 20 million boe per year.
		Oil production, refining and treatment and storage (downstream).	In England, Scotland and Wales:

		− The import of any of crude oil, intermediates, components and finished fuels. − The storage of any of crude oil, intermediates, components and finished fuels. − The production of intermediates, components and finished fuels through a range of refining or blending processes. − The delivery of petroleum-based fuels to retail sites, airports or end users.	Operators which provide or handle 500,000 tonnes of fuel per year. In Northern Ireland: Operators which have a storage capacity of greater than 50,000 tonnes of fuel.
	Gas	The function of supply (the sale or resale of gas) to consumers.	In England, Scotland and Wales: Gas suppliers (including aggregators where they act as suppliers) that meet the following two criteria (both must apply): • use of smart metering infrastructure; • supply greater than 250,000 consumers. In Northern Ireland: Licensed suppliers who supply to greater than 2,000 customers
		Gas (transmission) (downstream)	In England, Scotland and Wales: Network operators with the potential to disrupt supply to greater than 250,000 consumers. Operators of gas interconnectors with technical capacity greater than

			20mcm/d In Northern Ireland: The holder of a licence under Article 8(1)(a) of the Gas (NI) Order 1996.
		Gas (distribution).	In England, Scotland and Wales: Network operators with the potential to disrupt supply to greater than 250,000 consumers. For Northern Ireland: The holder of a licence under Article 8(1)(a) of the Gas (NI) Order 1996.
		Gas storage facilities supplying/storing gas for the national transmission network.	In England, Scotland and Wales: Operators with potential to input greater than 20mcm/d to the national transmission network. In Northern Ireland: The holder of a licence under Article 8(1)(b) of the Gas (NI) Order 1996.
		LNG system operators supplying/storing gas for the national transmission network.	In England, Scotland and Wales: Operators with potential to input greater than 20 mcm/d to the national transmission network. In Northern Ireland: The holder of a licence under Article 8(1)(d) of the Gas (NI) Order 1996.
		Gas (transmission) (upstream)	Operators with throughput of more than 20 million boe per year.
		Gas (production, refining and treatment)	Operators with throughput of more than 20 million boe per year.
Digital Infrastructure	n/a	Top Level Domain (TLD) Name Registries	Operators who service an average of 2 billion or more queries in 24 hours for domains registered within ICANN.

			Note: The threshold specified is an annual average and shall be based on the best available historic data from the preceding 12 months. Note: The threshold specified excludes growth of traffic load due to malicious activity such as DDoS attacks.
		Domain Name Services (DNS) Service Providers	Operators who provide DNS resolvers, offered for use by publicly accessible services, which service an average of 2,000,000 or more requesting DNS clients in 24 hours; or Operators who provide authoritative hosting of domain names, offered for use by publicly accessible services, servicing 250,000 or more different domain names. Note: The thresholds specified are an annual average and shall be based on the best available historic data from the preceding 12 months.
		Internet Exchange Point (IXP) Operators	Operators who have 50% or more annual market share amongst UK IXP Operators in terms of interconnected autonomous systems, or who offer interconnectivity to 50% or more of Global Internet routes. Note: Interconnected autonomous systems has the meaning set out in Article 4 (13) of the NIS Directive. Note: Global Internet routes means: The total number of active entries within the Global Internet Routing Table, averaged per calendar year.
Health Sector	Health care settings	Health care services.	Providers of non-primary NHS healthcare commissioned under the National Health Service Act 2006 as amended in England (but not including any individual doctors providing such healthcare).

			Local Health Boards and NHS Trusts in Wales (defined by the National Health Service (Wales) Act 2006). The 14 territorial Health Boards in Scotland; the following four special NHS Boards in Scotland: NHS National Waiting Times Centre, NHS24, Scottish Ambulance Service and The State Hospitals Board for Scotland; and Common Services Scotland (known as NHS National Services Scotland). Health and Social Care Trusts in Northern Ireland (defined by Health and Social Care (Reform) Act (Northern Ireland) 2009)
Transport	Air transport	Owner or operator of an aerodrome (as defined in Civil Aviation Act 1982).	Owner or operator of any aerodrome (i.e. airport) with annual terminal passenger numbers greater than 10 million.
		Provider of air traffic services (as defined in Transport Act 2000).	Any entity which is licensed to provide UK en-route air traffic services. Air traffic service providers at airports with annual terminal passenger numbers greater than 10 million.
		Air carriers (as defined in paragraph 4 of Article 3 of Regulation (EC) No 300/2008).	Air carriers with more than 30% of the annual terminal passengers at any individual UK airport that is in scope of the directive and more than 10 million total annual terminal passengers across all UK airports
	Maritime Transport	Harbour Authorities (as defined in the Merchant Shipping Act 1995).	Harbour Authorities or operators at ports with annual passenger numbers greater than 10 million. Or at ports that account for: - 15% of UK total Roll on-Roll off

		Operators of Vessel Traffic Services (as defined in Merchant Shipping (Vessel Traffic Monitoring and Reporting Requirements) Regulations 2004 SI 2004/2110).	(Ro-Ro) traffic; - 15% of UK total Lift on-Lift off (Lo-Lo) traffic; - 10% of UK total liquid bulk; or - 20% of UK biomass fuel.
		Operators of a port facility (as defined in Port Security Regulations 2009 – SI 2009/2048).	Operators of port facilities at ports that meet the above thresholds and that handle the type of freight specified in those thresholds.
		Passenger and freight water transport companies (as defined for maritime transport in Annex I to Regulation (EC) No 725/2004)	Operators that handle more than 30% of the freight at any individual UK port that is in scope and more than 5 million tonnes of total annual freight at UK ports. Operators that have more than 30% of the annual passenger numbers at any individual UK port that is in scope and more than 2 million total annual passengers at UK ports.
	Rail Transport	Operators of railway assets (as defined in section 6 of the Railways Act 1993) on the mainline railway network. This will include operators of trains, networks, stations and light maintenance depots, where operating those assets on the mainline railway network. Railway Undertaking as defined in the Northern Ireland Transport Act 1967.	Any operator of a railway asset on the mainline rail network (as defined).

		The mainline railway network will be defined to include all railways in GB but will exclude: i. International rail; ii. Metros, trams and light rail 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 activities not involving passenger or freight services for third parties.	
		Operators of railway assets (as defined in section 6 of the Railways Act 1993) for metros, trams and light rail (including underground) systems.	Operators with annual passenger journeys greater than 50 million.
		Operators of international rail services.	Any operator of a Channel Tunnel Train (as defined in the Channel Tunnel Security Order 1994). Any operator of international rail services in Northern Ireland, as defined in the Northern Ireland Transport Act 1967.
		International rail infrastructure managers	Any infrastructure manager of the Channel Fixed Link i.e. the Concessionaires (as defined in the Channel Tunnel Act 1987)

			Any infrastructure manager of international rail services in Northern Ireland, as defined in the Northern Ireland Transport Act 1967.
	Road Transport	Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962.	A road authority responsible for roads in the United Kingdom that annually in total have vehicles travelling more than 50 billion miles on them.
		Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council.	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.

Annex 2 - Updated list of proposed Competent Authorities

The Competent Authorities listed below are subject to final confirmation. The definitive list of Competent Authorities will be included in the NIS Regulations.

The Competent Authority in Northern Ireland will be confirmed by the Northern Ireland Government Departments.

The Government is working with the Scottish Government to determine the best arrangements for Competent Authorities in respect of devolved functions in Scotland, which will be confirmed in due course.

Sector	**Subsector**	**Competent Authority**
Drinking water supply and distribution	Not applicable	In England, the Secretary of State for Environment, Food and Rural Affairs (Defra), supported by the Drinking Water Inspectorate. In Wales, Welsh Ministers, supported by the Drinking Water Inspectorate.
Energy	Electricity	For England, Scotland and Wales, the Secretary of State for Business, Energy and Industrial Strategy and the Office of Gas and Electricity Markets (Ofgem).
	Gas (downstream)	For England, Scotland and Wales, the Secretary of State for Business, Energy and Industrial Strategy and the Office of Gas and Electricity Markets (Ofgem).
	Gas (upstream)	For England, Scotland and Wales, the Secretary of State for Business, Energy and Industrial Strategy, supported by the Health and Safety Executive.
	Oil (upstream)	For England, Scotland and Wales, the Secretary of State for Business, Energy and Industrial Strategy, supported by the Health and Safety Executive.
	Oil (downstream)	For England, Scotland and Wales, the Secretary of State for Business, Energy and Industrial Strategy, supported by the Health and Safety Executive.

Digital Infrastructure	Not applicable	The Office of Communications (Ofcom).
Health Sector	Health care settings	In England, the Secretary of State for Health supported by NHS Digital. In Wales, Welsh Ministers.
Transport	Air transport	The Secretary of State for Transport, acting jointly with the Civil Aviation Authority (CAA).
	Maritime transport	The Secretary of State for Transport.
	Road transport	In England and Wales the Secretary of State for Transport.
	Rail transport	In England and Wales, the Secretary of State for Transport,
Digital Service Providers	Cloud Services; online marketplaces; Search engines;	The Information Commissioner's Office (ICO).

Annex 3 - Proposed high level security principles

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

A.1 Governance:

- The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.

A.2 Risk Management:

- The organisation takes appropriate steps to identify, assess and understand security risks to network and information systems supporting the delivery of essential services. This includes an overall organisational approach to risk management.

A.3 Asset Management:

- Everything required to deliver, maintain or support networks and information systems for essential services is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).

A.4 Supply Chain:

- The organisation understands and manages security risks to the network and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.

Explanation

Governance: Effective security of network and information systems should be driven by organisational management and corresponding policies and practices. There should be clear governance structures in place with well-defined lines of responsibility and accountability for the security of network and information systems. Senior management should clearly articulate unacceptable impacts to the business (often called risk appetite), which should take into account the organisation's role in the delivery of essential services, so decision makers at all levels can make informed decisions about risk without constantly referring decisions up the governance chain. There should be an individual(s) who holds overall responsibility and is accountable for security. This individual is empowered and accountable for decisions regarding how services are protected. For small organisations, the governance structure can be very simple.

Risk Management: There is no single blueprint for cyber security and therefore organisations need to take steps to determine security risks that could affect the delivery of essential services and take measures to appropriately manage those risks.
Threats can come from many sources, in and outside the organisation. A good understanding of the threat landscape and the vulnerabilities that may be exploited is essential to effectively identify and manage risks. Such information may come from sources including NCSC, information exchanges relevant to the organisation's sector, and reputable government, commercial, and open sources, all of which can inform the

organisation's own risk assessment process. Organisations may contribute to the understanding of threats and vulnerabilities in their sector by participating in relevant information exchanges and liaising with authorities as appropriate.

There should be a systematic process in place to ensure that identified risks are managed and the organisation has confidence mitigations are working effectively. Confidence can be gained through, for example, product assurance, monitoring, vulnerability testing, auditing and supply chain security.

Asset Management: In order to manage security risks to the network and information systems of essential service organisations require a clear understanding of service dependencies. This might include physical assets, software, data, essential staff and utilities. These should all be clearly identified and recorded so that it is possible to understand what things are important to the delivery of the essential service and why.

Supply chain: If an organisation relies on third parties (such as outsourced or cloud based technology services) it remains accountable for the protection of any essential service. This means that there should be confidence that all relevant security requirements are met regardless of whether the organisation or a third party delivers the service. For many organisations, it will make good sense to use third party technology services. Where these are used, it is important that contractual agreements provide provisions for the protection of things upon which the essential service depends..

B) Proportionate security measures in place to protect essential services and systems from cyber-attack or system failures.

B.1 Service Protection Policies and Processes:

- The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support delivery of essential services.

B.2 Identity & Access Control:

- The organisation understands, documents and manages access to systems and functions supporting the delivery of essential services. Users (or automated functions) that can access data or services are appropriately verified, authenticated and authorised.

B.3 Data Security:

- Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause disruption to essential services. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the delivery of essential services. It also covers information that would assist an attacker, such as design details of networks and information systems.

B.4 System Security:

- Network and information systems and technology critical for the delivery of essential

services are protected from cyber-attack. An organisational understanding of risk to essential services informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.

B.5 Resilient Networks & Systems:

- The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation and management of systems that support the delivery of essential services.

B.6 Staff Awareness & Training:

- Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the delivery of essential services.

Explanation

Service Protection Policies and Processes: The organisation's approach to securing network and information systems that support essential services should be defined in a set of comprehensive security policies with associated processes. It is essential that these policies and processes are more than just a paper exercise and steps must be taken to ensure that the policies and processes are well described, communicated and effectively implemented.

Policies and processes should be written with the intended recipient community in mind. For example, the message or direction communicated to IT staff will be different from that communicated to senior managers. There should be mechanisms in place to validate the implementation and effectiveness of policies and processes where these are relied upon for the security of the essential service. Such mechanisms should also support an organisational ability to enforce compliance with policies and processes when necessary.

To be effective, service protection policies and processes need to be realistic, i.e. based on a clear understanding of the way people act and make decisions in the workplace, particularly in relation to security. If they are developed without this understanding there is a significant risk that service protection policies and processes will be routinely circumvented as people use workarounds and shortcuts to achieve their work objectives.

Identity & Access Control: It is important that the organisation is clear about who (or what in the case of automated functions) has authorisation to interact with the network and information system of an essential service in any way or access associated sensitive data. Rights granted should be carefully controlled, especially where those rights provide an ability to materially affect the delivery of the essential service. Rights granted should be periodically reviewed and technically removed when no longer required such as when an individual changes role or perhaps leaves the organisation.

Users, devices and systems should be appropriately verified, authenticated and authorised before access to data or services is granted. Verification of a user's identity (they are who they say they are) is a prerequisite for issuing credentials, authentication and access

management. For highly privileged access it might be appropriate to include approaches such as two-factor or hardware authentication.
Unauthorised individuals should be prevented from accessing data or services at all points within the system. This includes system users without the appropriate permissions, unauthorised individuals attempting to interact with any online service presentation or individuals with unauthorised access to user devices (for example if a user device were lost or stolen).

Data Security: The protection in place for data that supports the delivery of essential services must be matched to the risks associated with that data. As a minimum, unauthorised access to sensitive information should be prevented (protecting data confidentiality). This may mean, for example, protecting data stored on mobile devices which could be lost or stolen. Data protection may also need to include measures such as the sanitisation of data storage devices and/or media before sending for maintenance or disposal.

Protect data in accordance with the risks to essential services posed by compromises of data integrity and/or availability. In addition to effective data access control measures, other relevant security measures might include maintaining up-to-date back-up copies of data, combined with the ability to detect data integrity failures where necessary. Software and/or hardware used to access critical data may also require protection.

It is important to ensure that data supporting the delivery of essential services is protected in transit. This could be by physically protecting the network infrastructure, or using cryptographic means to ensure data is not inappropriately viewed or interfered with. Duplicating network infrastructure to prevent data flows being easily blocked provides data availability.

Some types of information managed by an OES would, if acquired by an attacker, significantly assist in the planning and execution of a disruptive attack. Such information could be, for example, detailed network and system designs, security measures, or certain staff details. These should be identified and appropriately protected.

(Note: data supporting the delivery of essential services must be identified in accordance with Principle A3 Asset Management).

System Security: There is a range of protective security measures that an organisation can use to minimise the opportunities for an attacker to compromise the security of networks and information systems supporting the delivery of essential services. Not all such measures will necessarily be applicable in all circumstances – each organisation should determine and implement the protective security measures that are most effective in limiting those opportunities for attackers associated with the greatest risks to essential services.

Opportunities for attackers to compromise networks and information systems, also known as vulnerabilities, arise through flaws, features and user error. Organisations should ensure that all three types of vulnerability are considered when selecting and implementing protective security measures.

Organisations should protect networks and information systems from attacks that seek to exploit software vulnerabilities (flaws in software). For example, software should be supported and up-to-date with security patches applied. Where this is not possible, other security measures should be in place to fully mitigate the software vulnerability risk.

Limiting functionality (e.g. disabling services that are not required) and careful configuration will contribute to managing potential vulnerabilities arising from features in hardware and software.

Some common user errors, such as leaving an organisation-issued laptop unattended in a public place, inadvertently revealing security-related information to an attacker (possibly as a result of social engineering) etc. can provide opportunities for attackers. Staff training and awareness on cyber security should be designed to minimise such occurrences (see B.6 Staff Training & Awareness).

Resilient Networks & Systems: The services delivered by an organisation should be resilient to cyber-attack. Building upon B.4 (the technical protection of systems), organisations should ensure that not only is technology well built and maintained, but consideration is also given to how delivery of the essential service can continue in the event of technology failure or compromise. In addition to technical means, this might include additional contingency capability such as manual processes to ensure services can continue.

Organisations should ensure that systems are well maintained and administered through life. The devices and interfaces that are used for administration are frequently targeted, so should be well protected. Spear phishing remains a common method used to compromise management accounts. Preventing the use of management accounts for routine activities such as email and web browsing significantly limits the ability for a hacker to compromise such accounts.

Staff Awareness & Training: Staff are central to any organisation's ability to operate securely. Therefore, operators of essential services should ensure that their employees have the information, knowledge, and skills they need to support the security of networks and information systems.

To be effective any security awareness and training programme needs to recognise and be tailored to reflect the way people really work with security in an organisation, as part of creating a positive security culture.

C) Appropriate capabilities to ensure network and information system security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.

C.1 Security Monitoring:

- The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the on-going effectiveness of protective security measures.

C.2 Proactive Security Event Discovery:

- The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the delivery of essential services even when the activity evades standard signature based security prevent/detect solutions (or when standard solutions are not deployed).

Explanation

Security Monitoring: An effective monitoring strategy is required so that actual or attempted security breaches are discovered and there are appropriate processes in place to respond. Good monitoring is more than simply the collection of logs. It is also the use of appropriate tools and skilled analysis to identify indicators of compromise in a timely manner so that corrective action can be taken.

This principle also indicates the need to provide effective and ongoing operational security. As time goes on new vulnerabilities are discovered, support arrangements for software and services change and functional needs and uses for technology change. Security is a continuous activity and the effectiveness of the security measures in place should be reviewed and maintained throughout the delivery and operational lifecycle of a system or service.

Anomaly Detection: Some cyber attackers will go to great lengths to avoid detection via standard security monitoring tools such as anti-virus software, or signature-based intrusion detection systems, which give a direct indication of compromise. Other, less direct, security event indicators may provide additional opportunities for detecting attacks that could result in disruption to essential services.

Examples of less direct indicators could include the following:

- Deviations from normal interaction with systems (e.g. user activity outside normal working hours).
- Unusual patterns of network traffic (e.g. unexpectedly high traffic volumes, or traffic of an unexpected type etc).
- ‘Tell-tale’ signs of attack, such as attempts to laterally move across networks, or running privilege escalation software.

It is not possible to give a generic list of suitable indicators since their usefulness in detecting malicious activity will vary considerably, depending on how a typical attacker’s actions might reveal themselves in relation to the normal operation of an organisation’s networks and information systems. Opportunities for exploiting these less direct security event indicators to improve network and information system security should be proactively investigated, assessed and implemented when feasible e.g. technically possible, cost effective etc. Successful attack detection by means of less direct security event indicators may depend on identifying combinations of network events that match likely attacker behaviour, and will therefore require an analysis and assessment capability to determine the security significance of detected events.

Wherever possible, network and information systems supporting the delivery of essential

services should be designed with proactive security event discovery in mind.

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

D.1 Response and Recovery Planning:

- There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential services in the event of system or service failure.
- Mitigation activities designed to contain or limit the impact of compromise are also in place.

D.2 Lessons Learned:

- When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.

Explanation

Response and Recovery Planning: Incidents will invariably happen. When they do organisations should be prepared to deal with them, and as far as possible, have mechanisms in place that minimise the impact on the essential service. The particular mechanisms required should be determined as part of the organisation's overall risk management approach. Examples might include things such as DDoS protection, protected power supply, critical system redundancy, rate-limiting access to data or service commands, critical data backup or manual failover processes.

Improvements: If an incident does occur it is important the organisation learns lessons as to why it happened and where appropriate takes steps to prevent the same issue from recurring. The aim should be to address the root cause or seek to identify systemic problems rather than solely fix a very narrow issue. For example to address the organisations overall patch management process rather than to just apply a specific missing patch.