Department for
Digital, Culture
Media & Sport

Security of Network and Information Systems

Public Consultation

August 2017
Department for Digital, Culture, Media and Sport

CONTENTS

1. How to respond

We welcome your views. To help us analyse the responses please use the online system wherever possible. Visit the Department's online tool to submit your response. Hard copy responses can be sent to:

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

The closing date for responses is 30 September 2017.

When providing your response, please also provide contact details - we may seek further information or clarification of your views.

This document is also provided in a Welsh language version. Should you require access to the consultation in another format (e.g. Braille, large font or audio) please contact us on 020 7211 6000 or niscallforviews@culture.gov.uk

Copies of responses, in full or in summary, may be published after the consultation closing date on the Department's website.

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.

If you want the information you provide to be treated confidentially, please be aware that, in accordance with the FOIA, public authorities are required to comply with a statutory code of practice which deals, amongst other things, with obligations of confidence. In view of this, it would be helpful if you could explain to us why you wish that information to be treated confidentially. If we receive a request for disclosure of that information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances.

2. Ministerial Foreword

Our modern economy, and the economic security it brings, are all themselves based on secure infrastructure. Network and information systems and the essential services they support play a vital role in society, from ensuring the supply of electricity, water, and health services, to the provision of passenger and freight transport.

Their reliability and security are essential to economic and societal activity, and the functioning of UK and European markets. Such systems can be a target for malicious actors that intend to damage or interrupt their operation through cyber attacks. Some systems may also be single points of failure for essential services and may be susceptible to other forms of compromise such as power failures, hardware failures and environmental hazards.

Adverse incidents affecting such systems could cause significant damage to the UK economy, impeding economic activity and undermining user confidence, or result in substantial financial losses. The magnitude, frequency and impact of network and information system security incidents is increasing. Recent events such as the WannaCry ransomware attack, the 2016 attacks on US water utilities, and the 2015 attack on Ukraine's electricity network clearly highlight the impact that can result from adversely affected network and information systems.

There is a need to therefore improve the security of network and information systems across the UK, with a particular focus on essential services (energy, health, transport, water, and digital infrastructure) which if disrupted, could potentially cause significant damage to the UK economy, society and individuals' welfare.

Network and information systems also play an essential role in facilitating the cross-border movement of goods, services and people. Given the transnational nature of some of the services provided using such systems, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect other countries as well as the UK.

The actions we propose to take in this consultation will help secure our infrastructure, and everything that relies on that infrastructure. This work to secure our network infrastructure is an important part of the government's work to prepare Britain for the future, and I look forward to your comments.

Rt Hon Matt Hancock MP
Minister of State for Digital

3. Introduction

As our reliance on technology grows, the impact of failure in those systems and the opportunities for those who would seek to compromise our systems and data increase. Responding to this threat and ensuring the safety and security of cyberspace 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 sets our vision for the UK in 2021 as secure and resilient to cyber threats, prosperous and confident in the digital world. To realise this vision we will work to achieve the following objectives:

- Defend: we have the means to defend the UK against evolving cyber threats. We are equipped to respond effectively to incidents. UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves;
- Deter: the UK will be a target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so;
- Develop: we have an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national requirements across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.

As part of the 'Defend' strand of the National Cyber Security Strategy the UK Government is working with our international partners to make sure the right regulatory framework is in place in the UK and Europe - one that incentivises better cyber security but avoids unnecessary business burdens.

The European Commission, in cooperation with Member States, have agreed a Directive with the aim of increasing the security of Network and Information Systems (NIS) within the European Union (EU). The Government supports the aims of the Directive and sets out below the proposed implementation approach in the UK.

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 this legislation will continue to apply in the UK.

It is important to note that the Government supports the overall aim of the NIS Directive and believes that strengthening the security of network and information systems supporting the UK’s essential service and digital service providers is consistent with the Government’s aim to ensure the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.

The Government’s intention is to implement this Directive through section 2(2) of the European Communities Act. The regulations will apply to the whole of the UK. In line with Article 1 (7) of the Directive, the banking and financial market infrastructures sectors within scope of the Directive will be exempt from aspects of the Directive where provisions at least equivalent to those specified in the Directive will already exist by the time the Directive comes into force. Firms and financial market infrastructure within these sectors must continue to adhere to requirements and standards as set by the Bank of England and/or the Financial Conduct Authority.

Although the Directive as a whole deals with reserved matters, elements of its implementation touch on matters that are the responsibility of the Devolved Administrations. Therefore the Devolved Administrations will be engaged separately, but at the same time as the consultation, to order to obtain their views.

This consultation also aims to seek views from industry, regulators and other interested parties on the Government's plans to transpose the Directive into UK legislation. It sets out the Government's proposed transposition approach and asks a series of questions on a range of detailed policy issues relating to transposition.

Following the consultation, the Government will analyse the feedback received and will issue a formal response within 10 weeks of the consultation closing date.

4. Essential services

The UK must identify the “operators of essential services” (OES) established in its territory for the purpose of this Directive. Operators designated as OES will be required to comply with the security and incident reporting requirements set out in the Directive.

According to the Directive an ‘operator of an essential service’ is a public or private entity that meets the following criteria:

- provides a service which is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information systems; and
- an incident affecting those systems would have significant disruptive effects on the provision of that service.

The Government’s proposed approach to determine these operators is to use the following four criteria:

- sector - the broad part of the UK’s economy;
- subsector - specific elements within an individual sector;
- essential service - the specific type of service;
- identification thresholds - criteria to identify essential operators (for example through size or the impact of events we are seeking to prevent).

A table of the proposed sectors, essential services, and identification thresholds can be found at **Annex 1**. The proposed thresholds are generally set at such a level as to capture only the most important operators in each sector based on the potential of a disruption to their essential service resulting in what the government considers would be a significant disruptive effect (separate thresholds will be established for incident reporting).

We have attempted to make these criteria as clear cut as possible to allow operators to identify whether they will need to comply with the Directive’s provisions. Each operator deemed to meet the criteria set by the Government will be designated as an OES and notified by the relevant competent authority. It will be for the Competent Authority and the relevant Government Department to determine the legal entity that will be designated under NIS and to ensure consistency in our approach across all sectors. It is important these thresholds are set at a level that enables essential service operators in all parts of the UK to be included. Unless otherwise indicated therefore, the proposed thresholds in Annex 1 are national thresholds. It may however be necessary to set separate thresholds for the Devolved Administrations, and if that is the case, further targeted consultations will be carried out as necessary.

In line with Recital 9 of the Directive the identification process for operators of essential services is not being carried out for the banking and financial market infrastructures sectors

within scope of the Directive given provisions at least equivalent to those specified in the Directive will already exist by the time the Directive comes into force.

The government is aware that there are a number of operators in certain sectors who, whilst not meeting the thresholds in Annex 1, are still considered to provide an essential service. In order to capture such smaller operators without broadening the scope of the Directive the Government is proposing to include a reserve power to designate specific operators in the implementing regulations outside of the thresholds in Annex 1.

This will be a limited power used only where the Government (or in future the relevant competent authority) assesses there are valid reasons for designation 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.

This power can only be used to designate operators that fall within one of the sectors in scope of the Directive. Any designation will have to be clearly justifiable, open to appeal, and clearly set out to the operator by the designating competent authority.

Questions

Q1 Are the identification thresholds set at a level that captures the most important operators in your sector based on their potential to cause a significant disruptive effect if disrupted? YES/NO

Q2 If not, why not? What would you change and why?
Narrative response?

5. National framework

The UK needs to put in place a framework of institutions to facilitate the operation of the Directive. The elements of this national framework include:

i. adopting a national strategy on the security of network and information systems;
ii. designating "one or more national competent authorities" to oversee implementation and compliance with the Directive's provisions;
iii. designating a "single point of contact" to act as a liaison point with other Member States; and
iv. creating one or more computer security incident response teams (CSIRTs).

i. National Strategy

"*The UK Cyber Security Strategy*" was published on 1 November 2016, which sets out how the UK will address cyber security challenges over the next five years. The UK Government is working closely with the Devolved Administrations on the strategy's application to Scotland, Wales and Northern Ireland. The UK's strategy is amongst the most comprehensive cyber strategies within the EU and we consider that it addresses most of the requirements of the Directive. Those requirements that are not covered by the current strategy can be addressed through a NIS specific addendum to the strategy. The Government therefore proposes to use this national strategy as our national strategy for the NIS Directive, and will include an addendum on NIS specific elements.

ii. Competent Authority

Every Member State is required to designate one (or more) NIS competent authority to be responsible for implementation of the Directive and for ensuring compliance with the Directive's provisions. Nominated competent authorities will be the main contact point for designated OES and digital service providers, and will be responsible for:

- publishing guidance on network and information security risk management and security measures;
- incident thresholds and reporting;
- taking decisions on whether to make incidents public,
- enforcement action where breaches of the Directive's provisions have been identified.

For OES under NIS, the appropriate competent authority will have the necessary means and powers to assess compliance with the Directive's requirements and to take action where necessary. Powers will include a power to obtain sufficient information in order to assess the level of network and information security. This can include the use of audits of OES relating to the security of network and information systems, conducted by the competent authority itself or a nominated audit agency. A competent authority will also have the power to issue binding instructions to OES to address issues relating to the security of network and information systems. These powers will not require an incident to have taken place. A Competent Authority will have the ability to delegate some of these tasks or responsibilities

to another organisation. However, unless there is existing legislation to provide for such a legal transfer of responsibility, ultimate responsibility will continue to remain with the Competent Authority.

The Government expects, and will encourage competent authorities and designated OES to engage in an on-going dialogue to address any concerns, with powers such as the power to direct being taken only as a last resort. Oversight of the NIS Directive is intended to be a proactive process, where regulators and operators work together to assess threats to the sector and agree the appropriate level of outcomes-based risk management required to counter the threat.

Approach to designating a NIS competent authority

There are two ways in which the UK's approach to transposition of the competent authority requirements could be taken forward:

1. nominating a single national competent authority, or
2. nominating multiple sector-based competent authorities

There are advantages and disadvantages to both approaches, with a balance needed between having expertise in the security of network and information systems, which a single competent authority may more easily develop, alongside a desire to ensure the nominated authority has a detailed understanding of the individual sectors and their associated challenges, something which multiple competent authorities approach may more easily facilitate.

The Government proposes to take a multiple competent authority approach. We consider that this is the most appropriate way to ensure that the security of network and information systems forms a central part of the mainstream regulation of each sector. The Government considers that there are significant benefits in having sector specific competent authorities that can use their knowledge and sectoral expertise to improve security in individual sectors. Sector specific regulators would also provide greater understanding of wider resilience issues and procedures for their individual sectors.

Where there are operators that provide essential services to more than one sector, and therefore fall under the remit of more than one competent authority, the relevant competent authorities will be encouraged to cooperate and provide consistent advice and oversight. We will also encourage this approach where an incident crossed regulatory boundaries (for example and NIS incident involving loss of personal data).

To support this approach, and provide nominated competent authorities with technical support, it is intended that the National Cyber Security Centre (NCSC) will have a significant supporting role, providing advice to competent authorities to enable them to undertake duties effectively. Ultimate authority and responsibility for any regulatory decision will lie solely with the competent authority.

Given the constitutional division of responsibilities between the UK Government and the Devolved Administrations, competent authority arrangements for each of the Devolved Administrations will also need to be in place. The Devolved Administrations are being

consulted separately on this.

The Government is proposing that the entities listed in **Annex 2** be designated as competent authorities for the NIS Directive. *Unless otherwise indicated, by geographical extent below, the proposed competent authorities will act for the whole of the UK*.

As reflected in some of the options above, details of who will take on the responsibilities of a competent authority in Northern Ireland, Scotland and Wales for those sectors that are not fully reserved matters, is still under discussion. Further details will be published once these roles are confirmed.

Competent Authorities for the banking and financial market infrastructures sectors are not being formally identified under this Directive. Firms and financial market infrastructure within these sectors must continue to adhere to requirements and standards as set by the Bank of England and/or the Financial Conduct Authority.

iii. Single Point of Contact

Each Member State is required to designate a single point of contact to act as a liaison on NIS matters within the EU and between different national competent authorities. The single point of contact's core tasks will include:

- preparing a summary report of incident notifications; and
- forwarding cross-border incidents to the single points of contact in other Member States.

The NCSC, as the UK's technical authority on cyber security issues, is proposed as the UK's Single Point of Contact.

iv. Computer Security Incident Response Team

Every Member State is required to designate one or more Computer Security Incident Response Teams (CSIRTs - also known as a Cyber Emergency Response Team or CERT) to be responsible for network and information system risk and incident handling. CSIRTs are to be responsible for:

- monitoring incidents at a national level;
- providing early warning, alerts and announcements;
- dissemination of information to relevant stakeholders about risks and incidents;
- responding to incidents;
- providing dynamic risk and incident analysis and situational awareness; and
- participating in the EU's CSIRTs network.

The UK already has a national Computer Emergency Response Team (CERT UK), which has been incorporated into the NCSC. Given the NCSC's existing role, we are proposing that the NCSC is designated as the UK's CSIRT under NIS. Where necessary, and to avoid disrupting existing reporting systems (for example NHS Digital), the NCSC will be able to delegate functions to existing CERTs. Where an incident relates to a non-cyber event, the

NCSC may not be able to provide incident response advice and the Competent Authority will be expected to take the lead, in co-operation with other relevant agencies.

Questions

Q3 Do you agree with the government's proposed approach of adopting a multiple competent authority model.
YES/NO

Q4 If not, why do you believe a single competent authority model represents a better option? Do you have an alternative outside of these two models?
Narrative answer.

Q5 Is the proposed competent authority for your sector a suitable choice?
YES/NO

Q6 If NO, who do you believe should be the competent authority for your sector and why?
Narrative answer.

6. Security requirements for operators of essential services

The NIS Directive requires that Member States ensure designated operators of essential services:

- take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems in the provision of their service; and
- take appropriate measures to prevent and minimise the impact of the incidents affecting the the security of the network and information systems used in the provision of their service.

The UK Government proposes to implement these provisions through a guidance and principles based approach, in which the Government will set out the high level security principles, which will be complemented by more detailed guidance, that will be either generic or sector specific. The high level principles will be set by the NCSC, in cooperation with Government departments and competent authorities. These principles describe the mandatory security outcomes that all operators will be required to achieve. The generic and sector specific guidance will be issued by the NCSC and competent authorities over time, and will be updated as necessary to reflect the nature of the threats to network and information systems.

The onus will be on the designated operators to demonstrate to the relevant competent authority that they are applying appropriate measures to manage the risks to their network and information systems. The operator will also be responsible for identifying the relevant network and information systems that will need to comply with the Directive's security requirements, agreeing these with the relevant competent authority who will have the final say. In order to help clarify what will be expected, the competent authority will over time publish and update guidance on :

- what the minimum is in terms of security expectations (e.g. level of responsibility, risk review etc.);
- what 'good' looks like for each sector; this must evolve as threats do; and
- a framework with which to determine the extent to which requirements are being met.

It is the Government's intention to publish this information over the following timeframe:

- Aug 2017: NCSC to publish the high level security principles all operators will be expected to comply with. This will be published as part of the public consultation.
- Jan 2018: NCSC to publish the generic cross-sector security guidance. This will supplement the high-level principles, and will assist and guide all operators regardless of sector.. This will include a Cyber Assessment Framework (CAF), which will provide a means with which to determine the extent to which requirements are being met
- Spring 2018: Competent authorities to indicate how OES should interpret the generic guidance and CAF for their own risk management procedures once the legislation

goes live in May.
- Nov 2018: Competent authorities to produce further detailed sector specific guidance, intended to reflect the unique circumstances of each sector, and which will be prepared in consultation with designated OES and with the support of the NCSC.

It is the UK Government's view that operators of essential services are responsible for managing their risks and will need to implement security measures in line with the high level principles established for the purposes of NIS, having regard to the more detailed sector-specific and generic guidance to be published by the relevant NIS competent authorities.

The Government wants to encourage a collaborative and proactive approach towards the security of network and information systems between the OES and the competent authority, so that competent authorities can be assured that risks are being effectively managed. It will be for the relevant competent authority to consider whether an operator has taken adequate measures to mitigate the risks posed to their network and information systems.

OES will be expected to meet the high level principles from the time that the legislation comes into effect (10 May 2018). Where there are difficulties, such as the implementation of measures will need more time, the OES is encouraged to speak with the Competent Authority to agree an appropriate timeframe for the necessary security measures to be put in place. OES will only be required to have regard to guidance that exists and is published, and where new guidance is put in place, OES should be given enough time to incorporate the new guidance into their risk management and security measures.

The high level security principles the Government proposes to establish are set out in **Annex 3**.

Operators of essential services will be expected to demonstrate that they have measures in place to meet the requirements of all of these principles, and the relevant competent authority will, as previously mentioned, have the powers to demand information relating to Operators' implementation and make judgements, and issue binding instructions, where they assess that those measures are not adequate.

Questions

Q7 Do you believe these high level principles cover the right aspects of network and information systems security to ensure that risks will be appropriately managed?
YES/NO

Q8 If NO, can you clarify what aspects you believe are missing and recommend how we could address these?
Narrative answer

Q9 Do you believe these principles would impose any additional costs on designated

operators, or on the sectors in scope as a whole?
YES/NO

Q10 If YES, what do you consider would be the anticipated resource implication on designated operators, or on the industry as a whole of meeting these principles? Are you able to elaborate on the nature of these costs? Where possible please detail any specific financial costs you consider would likely result.
Narrative answer

Q11 Do you have any plans to make additional security related investments as a result of this Directive? Where possible please indicate the size of investment (in £)?
YES/NO

Q12 If YES, please provide the amount and details of what investments would be required.
Narrative answer

7. Incident reporting for operators of essential services

The Directive requires designated OES to notify their relevant competent authority or CSIRT of incidents having a significant impact on the continuity of the essential services they provide. The purpose of NIS incident reporting is to provide the NCSC and relevant competent authority with information about disruptions to the continuity of an essential service. The NIS incident reporting requirements are not designed to replace the voluntary or mandatory frameworks that many Government departments and other organisations have established or may establish with industry, many of which have a much wider focus, either specifically on cyber or other concerns. The NIS requirements are intended to reinforce the reporting of certain types of incident, ensuring that competent authorities and the NCSC are aware of significant disruptions to the services provided by the sectors in scope where they are related to network and information systems. In some cases such reporting may be useful for the purposes of live incident management, and this will be encouraged where appropriate.

It is important to note that the NIS incident reporting requirements are not limited to "cybersecurity" incidents: any incident affecting the security of the network and information systems used for provision of the essential services may be reportable. This will include physical events where there is an impact on the security of a relevant network and information system. The inclusion of physical events is common to most international standards for cyber and network and information systems, such as ISO 27001, the NIST Framework and the Cloud Controls Matrix. For example, power failures, environmental hazards and hardware failures can be classed as NIS incidents as well as cyber attacks, malware, intrusions and viruses, provided that they have an adverse impact on network and information systems used to provide an essential service.

In this section, the UK Government sets out how it proposes:

- to define an incident for the purposes of NIS incident reporting;
- the thresholds for determining whether an incident has a significant impact; and
- the timeframe within which an incident must be reported;

The Government is aware of the burden that incident reporting can place on operators. In many of the sectors in scope of NIS, arrangements are already in place for OES to report incidents affecting essential services, something which has been encouraged for many years and in many cases is expected (although for many sectors this is not undertaken with legislative backing).

The Government is aiming therefore to align the NIS incident reporting requirements to existing arrangements where possible. Furthermore, in order to reduce bureaucratic burdens, all NIS incident reporting will be to one body, the NCSC as the dedicated Computer Security Incident Response Team (CSIRT) for the purposes of the Directive. The NCSC will be required to copy NIS incident reports to the relevant competent authority within each sector.

Defining an incident

The Directive states that a reportable incident is:

- Any event that has an actual adverse effect on the security of network or information systems used in the provision of essential services;
- where the security of network and information systems means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems; and
- One that has a significant impact on the continuity of essential services they provide.

The Government considers that there is an impact on continuity where there is a loss, reduction or impairment of an essential service.

The Government considers knowledge of threats and incidents to be an important part of developing a shared understanding of risks, and a vital part of reducing the overall threat to individual sectors and the UK as a whole. Therefore the Government proposes to encourage the voluntary reporting of incidents that do not meet the above thresholds, such as:

1. incidents where operators have to take action to maintain supply, provision, confidentiality or integrity of the service; and
2. incidents where software/intrusions are found that could potentially disrupt, or allow to be disrupted, the supply, provision, confidentiality or integrity of the service.

The voluntary reporting of such incidents will not subject OES to increased liability. However, competent authorities will expect an OES to respond to such incidents as part of their duty to ensure that appropriate risk-management measures are in place to mitigate the impact of any adverse incident. Engagement with the voluntary reporting systems (through NIS or other systems) will be considered as evidence that such measures are in place, in particular when considering the effectiveness of risk management and incident management systems.

Defining a significant impact

Thresholds for defining what constitutes a significant impact, will differ for each sector - what would constitute a significant impact for the health sector will be different from that of transport or energy. The government believes that the thresholds should be determined by the relevant competent authorities in consultation with OES and the NCSC. This process will begin following the end of this public consultation, when the identification thresholds and competent authorities have been determined.

Timeframe for incident reports

The NIS Directive does not specify a timeframe within which incidents meeting the NIS incident reporting thresholds should be reported. The Directive only states that operators

need to notify an incident “without undue delay”. However, in the event of an incident that may spread to other systems, sectors and countries, we consider it is important to report incidents at the earliest opportunity. It is common in similar regimes to set a maximum period in which companies have to report.

The Government believes that consistency with other legislative reporting requirements would be beneficial for OES. The Government therefore proposes that OES must report an incident “*without undue delay and as soon as possible, at a maximum no later than 72 hours after having become aware of an incident.*” Where existing arrangements for incident reporting relating to the loss of supply of the critical/essential service exist, and are of a shorter timeframe, these will remain in place.

The NIS incident reporting requirements are not intended to take the place of OES seeking advice and support from the NCSC or the competent authority in the event of an incident. It is expected that designated OES will engage with the NCSC and competent authority throughout an incident and will comply with requests for information by the competent authority.

Questions

Q13 Do you consider these incident reporting proposals to be reasonable to ensure that serious incidents affecting the network and information systems of essential services are reported?
YES/NO

Q14 If NO, why not? Can you suggest revised incident reporting proposals that ensure serious incidents are reported?
Narrative answer

Q15 Do you consider that the proposed timeframe for providing incident reports place an undue burden on designated operators of essential services?
YES/NO

Q16 If YES, can you explain what these burdens and costs would be?
Narrative answer

8. Digital service providers (DSP)

The NIS Directive also applies, in a lighter touch manner, to three types of Digital Service Providers. It is regarded as lighter touch because regulation and enforcement can only be applied after an incident or if a company is reported to the competent authority to be non-compliant with the Directive. It is important to note that Digital Service Providers that employ fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed €10 million are automatically excluded from the scope of the NIS Directive.

In the event of a reportable incident, the appropriate competent authority will have the power to obtain sufficient information in order to assess the level of security of network and information systems in order to make a judgement about whether the DSP took adequate precautions in line with the requirements of the NIS Directive.

Definition of a DSP

The NIS Directive defines DSPs as the following:

1. *Online marketplaces*
2. *Online search engines*
3. *Cloud computing services*

In order to clearly identify companies that will fall within scope of the Directive, the Government proposes to use the following definitions in its advice to the competent authority and industry:

Online marketplaces

- An online marketplace is defined as a platform that acts as an intermediary between buyers and sellers, facilitating the sale of goods and services. Online marketplaces are only in scope if sales are made on the platform itself. Sites that redirect users to other services to make the final transaction (e.g. price comparison sites) are not in scope. Sites that only sell directly to consumers are not in scope (e.g. online retailers).

Online search engines

- ‘online search engine’ means a digital service that allows users to perform searches of 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. Where a site offers search engine facilities, but those facilities are powered by another search engine, then the underlying search engine is required to meet the requirements of the NIS Directive.

Cloud computing services

- ‘cloud computing service’ means any company that offers:
    - “‘Infrastructure as a Service’ (IaaS). IaaS refers to the delivery of virtualised computing resource as a service across a network connection, specifically hardware – or computing infrastructure - delivered as a service. Offerings

include virtualised server space, storage space, network connections and IP addresses. The resource is pulled from a pool of servers distributed across data centres under the provider's control, the user is then granted access to this resource in order to build their own IT platforms.

- ‘Platform as a Service’ (PaaS) services provide developers with environments on which they can build applications that are delivered over the internet, often through a web browser.
- Business to Business ‘Software as as Service’ (SaaS). SaaS is a software delivery model in which applications are hosted (usually by a provider) and made available to customers over a network connection, and where the application will not work if the Service provider has a failure. SaaS providers offering services for entertainment purposes only are not included.

Questions

Q17 Are Digital Service Providers easily able to identify themselves using these criteria?
YES/NO

Q18 If NO, Why Not? Can you provide revised criteria that would identify providers more easily?
Narrative answer

Q19 Would using these definitions create any unfair competitive advantage or disadvantage for Digital Service Providers within scope?
YES/NO

Q20 If you answered YES to the previous answer , please clarify nature of the advantage or disadvantage?
Narrative answer

Security requirements for DSPs

The Directive requires that DSPs identify, and take appropriate and proportionate technical and organisational measures, to manage the risks posed to their security of network and information systems. This covers:

A. the security of systems and facilities;
B. incident handling;
C. business continuity management;
D. monitoring, auditing and testing;
E. compliance with international standards.

The Government again proposes to follow a principles and guidance approach to security measures for Digital Service Providers, with the guidance closely linked to that provided by the European Network and Information Security Agency (ENISA). Compliance with European guidelines will be a requirement for access to the Single Market, therefore the

Government will aim to ensure that the UK's guidance is a close to ENISA's guidance as possible.

It is the responsibility of the European Commission to set the framework for incident reporting for DSPs under NIS, in cooperation with Member States. This framework has not yet been set and the European Commission will produce an Implementing Act (legally binding guidance) establishing this framework by 9 August 2017.

For the UK, our high level security principles for DSPs will be as closely aligned to these requirements, and the requirements of the General Data Protection Regulation (GDPR) as possible in order to reduce burdens on business. We propose that our high level principles be based along the following lines:

A. proportionate security measures in place to protect services and systems from cyber-attack or systems failure;
B. appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage incidents;
C. capabilities to minimise the impacts of a cyber security incidents on the delivery of services including the restoration of those services;
D. capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, services;
E. measures in place are, where possible, compatible or comparable to internationally recognised cyber security standards.

Further clarification of these principles, and the underlying guidance will be developed once the European Commission publicises its Implementing Act, in co-operation with the Information Commissioner's Office as the UK's national supervisory authority for GDPR and the NCSC.

Questions

Q21 Are these principles reasonable?
YES/NO

Q22 If NO, Why Not? Can you suggest revised principles that would enable important incidents to be reported?
Narrative answer

Q23 What would be the impact on your business in applying these principles?
Narrative answer

Q24 Do you have an alternative preferred approach?
Narrative answer

Incident Reporting

The Government proposes to mirror our approach to incident reporting for Digital Service Providers, with that of Essential Services, within the limits set out by the Directive for Digital Service Providers. Our aim is to have an incident reporting threshold based around the following principles:

- that impacts supply, provision, confidentiality or integrity of the service;

It is the responsibility of the European Commission to set the framework for incident reporting for DSPs under NIS, in cooperation with Member States. This Framework has not yet been set and the European Commission will produce an Implementing Act establishing this framework over the summer.

In the event of an incident, it is important that DSPs are required to report as soon as possible, and it is common in similar regimes to set a maximum period in which companies have to report. The NIS Directive does not specify a timeframe, only stating that operators need to notify about an incident "without undue delay".

The Government is proposing that companies must report an incident "*without undue delay and as soon as possible, at a maximum no later than 72 hours after having become aware of it.*" This will ensure that incident reporting under NIS is consistent with GDPR to minimise regulatory burdens of different approaches.

Given the uncertainty at this stage on the level of detail of security and incident reporting requirements for DSPs, it is difficult to consult effectively on their impact at this time. The Government therefore proposes that once these aspects have been clarified that it carries out a smaller, targeted consultation. If you wish to be a part of this smaller consultation exercise, please provide appropriate contact details.

Questions

Q25 Would this incident reporting timeframe place an undue burden on your business or operations?
YES/NO

Q26 If YES, can you explain what these burdens and costs would be?
Narrative answer

Q27 Do you wish to take part in the proposed targeted consultation exercise once the security and incident reporting thresholds have become clearer?
YES/NO

Q28 If YES, please provide an appropriate name, and email address for future correspondence.

9. Penalty regime

Penalties

Member States are required to lay down the rules on penalties applicable to infringements of the national provisions adopted pursuant to this Directive and must take all measures necessary to ensure that they are implemented. Any penalties provided for in national legislation should be effective, proportionate and dissuasive.

The UK Government's approach to new regulation is that all Governments should ensure that regulations are necessary, fair, effective, affordable and enjoy a broad degree of public confidence.

Given the theoretically high impact of a loss of an "essential service", including possible loss of life (not all services) or major economic loss to associated industry or regions, the Government believes that the NIS Directive needs to set a high bar for the maximum level of penalty. The Government therefore proposes to adopt an approach for the penalty regime for NIS similar to that of the General Data Protection Regulation (GDPR). This will provide consistency in the Government's regulatory approach towards overall cyber security.

The Government proposes to have two bands of penalties under the NIS Directive:

- Band one - set at a maximum €10m or 2% of global turnover - for lesser offences, such as failure to cooperate with the competent authority, failure to report a reportable incident, failure to comply with an instruction from the competent authority.

- Band two - set at a maximum of €20m or 4% (whichever is greater) - for failure to implement appropriate and proportionate security measures.

The Government understands that it is not possible to fully protect any information systems from security incidents - be they hardware failure or external attack. An OES or DSP's approach to implementing improvements based on the principles set out in this document will be a clear mitigation for any subsequent penalty. The role of the competent authority in the event of any incident will be to assess whether the incident was foreseeable, whether effective risk management was in place, and whether the operator (or digital service provider) had appropriate security measures in place.

Financial penalties should only be levelled as a last resort where it is assessed appropriate risk mitigation measures were not in place without good reason. In addition, the penalties listed above are maximum penalties, for use in the most egregious incidents, and it is expected that mitigating factors including sector-specific factors will be taken into account by the competent authority when deciding appropriate regulatory response.

In the event of any enforcement action by the competent authority, the competent authority will notify the operator of impending action, allow the operator an opportunity to make representations, and confirm the final decision and reasoning of the competent authority.

Decisions taken by the competent authority will be enforceable by civil proceedings, and appealable through the court system.

Questions

Q29 Do you consider the proposed penalty regime to be proportionate to the risk of disruptions to operators of essential services?
YES/NO

Q30 Do you believe that the proposed penalty regime will achieve the outcome of ensuring operators take action to ensure they have the resources, skills, systems and processes in place to ensure the security of their network and information systems?
YES/NO

Q31 If you answered NO to either of these two questions, please explain how the penalty regime could be amended to address your concerns.
Narrative answer

Annex 1 - Table of essential services and identification thresholds

The UK must identify the “operators of essential services” (OES) established in its territory. Unless otherwise indicated, these are national thresholds that apply to the whole of the UK. The proposed thresholds are generally set at such a level as to capture only the most important operators, rather than the whole sector. Please note that operators may also be designated using the reserve designation power. See page 7 for further details.

Sector	Subsector	Essential service	Identification thresholds
Drinking water supply and distribution	n/a	The supply of potable water to households.	Operators with sites serving 350,000 or more people.
Energy	Electricity	The function of supply (the sale or resale of electricity) to consumers.	Electricity suppliers (incl. aggregators where they act as suppliers) that meet the following two criteria (both must apply): ● use of smart metering infrastructure; ● supply > 250,000 consumers. Operators of electricity generators* with a generating capacity ≥ 2 Gigawatts (GW), including: ● Standalone transmission connected generation; ● Multiple generating units with a cumulative capacity ≥ 2 Gigawatts (GW) controlled by an individual/common control network; *excluding nuclear electricity generation. The government does not consider the civil nuclear sector to be in scope of the NIS Directive; For Northern Ireland, Northern Ireland officials have proposed separate NI specific thresholds: Licensed suppliers who: (i) supply to large industrial/commercial customers; or (ii) supply to > 8,000 customers And any generator with a

			generating capacity ≥ 400MW
		Electricity (SEM Operator)	The holder of a SEM operator licence under Article 8(1)(d) of the Electricity (NI) Order 1992* *this will be the subject of engagement with the Department of Communications, Climate Action and Environment in the Republic of Ireland during the consultation period.
		Electricity (transmission).	Network operators with the potential to disrupt supply to > 250,000 consumers. International interconnectors and Direct Current converter station with a capacity greater ≥ 1 Gigawatts (GW). In Northern Ireland, holders of a transmission licence under Article 8(1)(b) of the Electricity (NI) Order 1992
		Electricity (distribution)	Network operators with the potential to disrupt supply to > 250,000 consumers. In Northern Ireland, holder of a distribution licence under Article 8(1)(bb) of the Electricity (NI) Order 1992.
	Oil	Oil transmission (upstream). The operation of an "upstream petroleum pipeline" as defined in the Energy Act 2011 (90)(1).	Operators with throughput of more than 20 million barrels of oil equivalent (boe) of oil per year.
		Oil transmission (downstream). The distribution of	Operators which provide or handle 500,000 tonnes of fuel/per year. For Northern Ireland, Northern

		petroleum-based fuels to other storage sites throughout the UK by road, pipeline, rail or ship.	Ireland officials have proposed separate NI specific threshold of 50,000 tonnes of fuel/per year:
		Oil production, refining and treatment and storage (upstream). The operation of "oil processing operations" as defined in the Energy Act 2011(90)(2).	Operators with throughput of 20 million boe of oil per year.
		Oil production, refining and treatment and storage (downstream). − 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 distribution of petroleum-based fuels to other storage sites throughout the UK by road, pipeline, rail or ship. − 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. For Northern Ireland, Northern Ireland officials have proposed separate NI specific threshold of 50,000 tonnes of fuel/per year:
	Gas	The function of supply (the sale or resale of gas) to consumers.	Gas suppliers (incl. aggregators where they act as suppliers) that meet the following two criteria (both must apply):

			• use of smart metering infrastructure; • supply > 250,000 consumers. For Northern Ireland, Northern Ireland officials have proposed separate NI specific thresholds: Licensed suppliers (i) supply to large industrial/commercial customers; or (ii) supply to > 2,000 customers
		Gas (transmission).	Network operators with the potential to disrupt supply to > 250,000 consumers. For Northern Ireland, holders of a licence under Article 8(1)(a) of the Gas (NI) Order 1996
		Gas (distribution).	Network operators with the potential to disrupt supply to > 250,000 consumers. For Northern Ireland, holders 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.	Operators with potential to input > 20-30mcm/d to the national transmission network. For Northern Ireland, holders 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.	Operators with potential to input > 20-30mcm/d to the national transmission network. For Northern Ireland, holders of a licence under Article 8(1)(d) of the Gas (NI) Order 1996.
		The operation of an "upstream petroleum pipeline" as defined in the	Operators with throughput of more than 20 million boe of gas per year.

		Energy Act 2011 (90)(1).	
		The operation of a "gas processing operation" as defined in the Energy Act 2011(90)(2).	Operators with throughput of more than 20 million boe of gas per year.
Digital Infrastructure	n/a	Top Level Domain (TLD) Name Registries	Operators who service an average of 2 billion queries or more in 24 hours.
		Domain Name Services (DNS) Service Providers	Operators who provide DNS resolution and who service an average of 60 million queries or more in 24 hours.
		Internet Exchange Point (IXP) Operators	Operators who provide a total port capacity of 5 Tbps (terabits per second) or more.
Health Sector	Health care settings	NHS Trusts and Foundation Trusts in England (defined by the NHS Act 2006). Local Health Boards and NHS Trusts in Wales (defined by the National Health Service (Wales) Act 2006).. NHS Boards in Scotland. Health and Social Care Trusts in Northern Ireland (defined by Health and Social Care (Reform) Act (Northern Ireland) 2009)	All.
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 licenced 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).	At ports with annual passenger numbers greater than 10 million. At ports that account for: - 15% of UK total Roll on-Roll off (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 Vessel Traffic Services (as defined in Merchant Shipping (Vessel Traffic Monitoring and Reporting Requirements) Regulations 2004 SI 2004/2110).	
		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.
		Water Transport Companies (Definition needed).	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 any railway asset (as defined in section 6 of the Railways Act 1993) on the national rail network or the Northern Ireland Transport Act 1967. (Includes operators of trains, networks, stations and light maintenance depots). Does not apply to operator of trains or networks reserved for local, historical or touristic use.	Any operator of a railway asset on the national rail network.
		Operators of guided transport systems (as defined in section 2 of the Railways and other Guided Transport Systems Safety Regulations 2006).	Operators with annual passenger numbers 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.	Road authority or operator of Intelligent Transport Systems for a road network that has greater than 50 billion annual motor vehicle miles. For Northern Ireland, Northern Ireland officials have proposed a separate approach which will include the Northern Ireland Roads Authority.
		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.	

Annex 2 - Table of proposed competent authorities

We are engaging with Northern Ireland to consider who is best placed to act as competent authority for the relevant devolved sectors in Northern Ireland. As such, for those areas that are devolved in Northern Ireland, we have not included proposals for a Competent Authority in the table below.

Sector	**Subsector**	**Proposed Competent Authority**
Drinking water supply and distribution	Not applicable	For England we propose that the Department for Environment, Food and Rural Affairs (Defra) is nominated as the competent authority. In Wales, the Cabinet Secretary for Environment and Rural Affairs has agreed to nominate Welsh Ministers as the Competent Authority for the water sector in Wales subject to clarification of funding to facilitate the UK Government transposition of the EU Security of Networks and Information Systems (NIS) Directive into UK law. For Scotland, we are consulting with the Scottish Government on who should be the appropriate competent authority.
Energy	Electricity	For England, Scotland and Wales, we propose that the Secretary of State, Department for Business, Energy and Industrial Strategy (BEIS) is nominated as the competent authority. We are exploring whether certain functions could be delegated in whole or part to the Office of Gas and Electricity Markets (Ofgem).
	Gas (downstream)	For England, Scotland and Wales, we propose that the Secretary of State, BEIS is nominated as the competent authority. We are exploring whether certain functions could be delegated in whole or part to Ofgem.
	Gas (upstream)	For England, Scotland and Wales, we propose that the Secretary of State, BEIS is nominated as the competent authority. We

		are exploring whether certain functions could be delegated to industry relevant bodies.
	Oil (upstream)	For England, Scotland and Wales, we propose that the Secretary of State, BEIS is nominated as the competent authority. We are exploring whether certain functions could be delegated to industry relevant bodies.
	Oil (downstream)	For England, Scotland and Wales, we propose that the Secretary of State, BEIS is nominated as the competent authority. We are exploring whether certain functions could be delegated to industry relevant bodies.
Digital Infrastructure	Not applicable	Office of Communications (Ofcom).
Health Sector	Health care settings	For England we propose that the Department of Health be designated as the competent authority, with some functions and responsibilities delegated to NHS Digital. In Wales, the Cabinet Secretary for Health, Well-being and Sport has agreed to nominate Welsh Ministers as the Competent Authority for the health sector in Wales subject to clarification of funding to facilitate the UK Government transposition of the EU Security of Networks and Information Systems (NIS) Directive into UK law. For Scotland, we are consulting with the Scottish Government on who should be the appropriate competent authority.
Transport	Air transport	The Secretary of State, Department for Transport (DfT), with some functions delegated to the Civil Aviation Authority (CAA).

	Maritime transport	The Secretary of State, DfT.
	Road transport	For England we propose that the Secretary of State, DfT be designated as the competent authority. In Wales, the Cabinet Secretary for Economy and Infrastructure has agreed to nominate Welsh Ministers as the Competent Authority for the road transport sector in Wales subject to clarification of funding to facilitate the UK Government transposition of the EU Security of Networks and Information Systems (NIS) Directive into UK law. For Scotland, we are consulting with the Scottish Government on who should be the appropriate competent authority.
	Rail transport	For rail transport in Great Britain, we propose to designate the Secretary of State, DfT as the competent authority.
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:

- There are appropriate management policies and processes in place to govern the organisations 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:

- All systems and/or services that are required to maintain or support essential services are 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 must 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. 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 security of network and information systems 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. There is an expectation that organisations would take steps to understand the types of threats that might be relevant to them, and share information about the threats facing them with appropriate authorities. This includes thinking about who might conduct an attack, or key single points of failure that need protection. Examples could include online attackers, 'insider' threats or accidental threats. There should be efforts to seek an understanding of potential system vulnerabilities that the identified threats might attempt to take advantage of. This might include technical vulnerabilities, misuse of legitimate business processes or anything else that could impact the essential service. There should be a systematic process in place to ensure that identified risks are managed and the

organisation has confidence in the efficacy of the applicable mitigations.

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, utilities and so on. 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) they remain accountable for the protection of any essential service. This means that there should be confidence that the security principles 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 and communicates appropriate policies and processes that direct the overall organisational approach to securing systems and data that support delivery of essential services.

B.2 Identity & Access Control:

- The organisation understands, documents and controls access to systems and functions supporting the delivery of essential services. Rights or access granted to specific users or functions should be understood and well managed.
- Users (or automated functions) that can access data or services are appropriately verified, authenticated and authorised.

B.3 Data Security:

- The organisation prevents unauthorised access to data whether through unauthorised access to user devices, interception of data in transit or accessing data that remaining in memory when technology is sent for repair or disposal.

B.4 System Security:

- Network and information systems and technology critical for the delivery of essential services are protected from cyber-attack. This includes minimising the opportunity for attack by configuring technology well, actively managing software vulnerabilities, minimising services available, and controlling connectivity and physical access.

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 are given appropriate support to ensure they can support the security of network and information systems 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 organisational 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 aim of the policy or process is effectively implemented.

Policies and processes should be well described and communicated. Steps should be taken to ensure that intended recipients understand the policy or process and are practically able to follow its direction. Policies and processes should be written with a clear understanding of the intended recipient community. 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.

Identity & Access Control: It is important that the organisation has clarity on who (or what in the case of automated functions) is authorised 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: Mobile devices will get lost or stolen from time to time. When this occurs, it is important that such loss does not lead to compromise of data stored on the device. Data at rest on the device would typically be protected either physically or through technical means such as encryption. All technology and memory components should be managed through its entire lifecycle including appropriately sanitising information from memory prior sending technology for repair or disposal. It is important to ensure that sensitive data is protected whilst in transit either by physically protecting the network infrastructure or preventing it from being read or interfered with via cryptographic means. This may mean using options such as an appropriate VPN for remote access or TLS when providing a

web presentation of data or services.

System Security: Network and information systems must be protected from attacks that seek to exploit software vulnerabilities. Organisations should minimise the opportunity for successful attack by limiting software and associated permissions to those needed for legitimate functions. Software should be supported and up to date with security patches applied. Where patching is technically problematic there are other possible mitigations but these should be viewed as sub-optimal and care must be taken to ensure that they are effective.

It is important that arbitrary software cannot interact with network and information systems supporting essential services or access sensitive data. There should be control exercised over what software or apps can be installed, or user installed software or apps should be technically prevented from interacting with services or data. Steps should be taken to manage the risk of malware ingress through import of data via both network connections and any removable media used.

All hardware and software should be well configured by for example disabling services that are not required and by changing default passwords. Connectivity to, and interfaces/APIs presented by systems critical to the essential service should be highly constrained. This minimises the opportunity for an attacker to discover and exploit any given vulnerability. Devices and technical infrastructure should be protected from physical interference or tampering that could undermine the security of network and information systems. For larger organisations with their own network infrastructure, steps should be taken to prevent unauthorised devices from accessing the network, for example by use of well configured corporate WiFi, device authentication and disabling network ports by default

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

Organisations should ensure that network and information systems are well maintained and administered through life. The devices and interfaces that are used for administration are frequently themselves the target for cyber-attack. Spear phishing campaigns remain 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: An organisation’s staff should be considered the first line of defence. They should be given appropriate support such as training and the correct policies, processes and technical tools to discharge their roles efficiently without having to resort to unofficial IT or break defined rules.

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 Anomaly Detection:

- The organisation detects anomalous events in the network and information systems affecting, or with the potential to affect, the delivery of essential services.

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 to such. Good monitoring is more than simply the collection of logs, but the use of appropriate tools and skilled analysis to correlate events and discover anomalous activity.

This principle also indicates the need to provide effective and on-going 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. It is important that security is considered a continuous activity and the effectiveness of the security measures in place is assured throughout the delivery and operational lifecycle of a system or service.

Anomaly Detection: There should be activity that aims to detect deviation from 'normal'. This refers to technology, business processes and the operation of the essential service. The first challenge that must be addressed to meet this principle is taking steps to define what 'normal' is for the organisation. This might be in the context of access to sensitive data or the operation of the essential service. With a contextualised understanding of 'normal' the organisation should take steps to detect when activity falls outside of these bounds and take corrective action.

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 are in place that are designed to contain or limit the impact of compromise.

D.2 Improvements:

- When an incident occurs, steps must be taken to understand the root cause of that incident and take appropriate remediating action.

Explanation

Response and Recovery Planning: Incidents will invariably happen, so when they do organisations should be prepared to deal with those incidents and as far as possible have mechanisms in place that minimise the impact on the essential service. The particular mechanisms required will be determined by organisations for themselves as part of their 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 reoccurring. 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.