



UK Government

Critical Undersea Infrastructure Security and Resilience: Proposals for modernising the UK's legislation

October 2026

CP 1683



Government of the United Kingdom
Department for Digital, Culture, Media & Sport

Critical Undersea Infrastructure Security and Resilience: Proposals for modernising the UK's legislation

Presented to Parliament by the Minister of State for Digital, Culture,
Media and Sport and the Minister of State for Energy Security and Net Zero
by Command of His Majesty

October 2026



© Crown copyright, 2026

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at

Department for Digital, Culture, Media and Sport

100 Parliament Street

London SW1A 2BQ

Email: enquiries@dcms.gov.uk

Tel: 020 7211 6000

ISBN 978-1-5286-6814-9

E03683331 10/26

Printed on paper containing a minimum of 40% recycled fibre content

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office.

Contents

Joint Ministerial Foreword	5
Executive Summary	6
Chapter 1: Introduction	10
The infrastructure and why it matters	10
Security and resilience risks	11
Rationale for legislation	11
Structure of this White Paper	12
Chapter 2: Key Terms	13
Subsea conveyance systems and services	13
Providers	14
Security compromise	14
Chapter 3: Criminal penalties regime	15
Background	15
Objectives	15
Overview of proposals	16
Infrastructure in scope	16
New offences	16
Penalties and liability	17
Territorial extent	19
Enforcement	20
Chapter 4: Security and Resilience Duties	22
Background	22
Objectives	23
Overview of proposals	23
Duties on providers	24
Secondary legislation and codes of practice	26
Entities, systems and services in scope	26
Territorial extent	28
Monitoring and enforcement	28

Chapter 5: National Security Direction Power	30
Background	30
Objectives	30
Overview of proposals	31
Entities in scope	31
Direction power	32
Territorial extent	35
Monitoring and enforcement	36
Chapter 6: Regulation of Sensing Technologies	38
Background	38
Objectives	39
Overview of proposals	39
Scope	39
Regulatory regime	41
Screening regime	41
Baseline security requirements	43
Territorial extent	45
Monitoring and enforcement	46
Annex A: How to respond and next steps	48
Annex B: Consultation Questions	49

Joint Ministerial Foreword



The first duty of government is to keep the country safe. Today, that means protecting not only our borders, but the critical infrastructure beneath our seas.

Subsea cables carry approximately 99% of the UK's international data traffic, underpinning many of the digital services on which modern life depends. Likewise, our subsea pipelines and interconnectors are critical for powering our economy with secure and increasingly clean power. This critical undersea infrastructure (CUI) is highly resilient. When faults occur, they tend to pass entirely unnoticed by the public. That resilience reflects decades of investment and cooperation between industry and government.

However, the risks are evolving. In April, the Defence Secretary John Healey revealed that our Armed Forces – in partnership with our allies – tracked Russian submarines whose mission was to survey cables. Such activity raises serious questions about the security and resilience of CUI globally, and the need for modern legal frameworks to protect it.

The Parliamentary Joint Committee on the National Security Strategy (JCNSS) has been clear that UK legislation has failed to keep pace with the growing importance of CUI, or the risks it now faces. We agree with the Committee. The principal offence for damaging subsea cables dates back to 1885, refers to 'telegraphic' communications, and makes limited provision for energy infrastructure. It fails to provide a satisfactory deterrent.

To address such deficiencies, the government has undertaken a comprehensive review of the effectiveness of UK legislation in managing the risks to CUI. This White Paper reflects the findings of that review, with a new set of proposals to modernise our legislation. It includes proposals for: new criminal offences and penalties for those who damage CUI; new security and resilience duties for owners and operators of subsea telecoms cable infrastructure; new national security powers for government to direct action; and a new security framework for subsea sensing technologies.

We encourage everyone with an interest in these proposals – particularly CUI providers and maritime and fishing organisations – to engage with this consultation. Your views will help ensure any new legislation is appropriate and proportionate, helping us protect the infrastructure on which the UK depends.

A handwritten signature in black ink, reading 'Ian Murray'.

Ian Murray MP

Minister of State, Department for Digital,
Culture, Media and Sport

A handwritten signature in black ink, reading 'Michael Shanks'.

Michael Shanks MP

Minister of State, Department for Energy
Security and Net Zero

Executive Summary

1. As an island nation, the United Kingdom relies on subsea telecoms cables, pipelines, interconnectors and other offshore energy infrastructure to meet its data and energy needs, and our dependence on this critical undersea infrastructure (CUI) continues to increase.
2. Growing demand for artificial intelligence, cloud computing and other data-intensive technologies is driving a continuing need for high-capacity international connectivity. Energy generation and transmission is becoming increasingly decentralised and maritime based as we transition to clean power and net zero. Consequently, CUI is becoming ever more central to the functioning of modern society, making its continued security and resilience increasingly important to the UK's future prosperity and security.
3. The UK's subsea connectivity has proved resilient, with infrastructure faults rarely causing noticeable disruption to our access to the internet or energy supplies. However, CUI remains inherently vulnerable to damage. Much of it lies unprotected on, or just below, the seabed and comes ashore at a relatively small number of strategically important landing sites.
4. The UK's National Security Strategy notes that the threats to the homeland from state actors are increasing and critical national infrastructure, including undersea cables and pipelines, will continue to be a target. Deliberate interference can be difficult to distinguish from accidental damage, creating opportunities for hostile actors to obscure attribution and reinforcing the importance of maintaining effective deterrence, security and resilience.
5. Commercial incentives and voluntary arrangements alone will not ensure sufficient levels of CUI security and resilience to mitigate these risks. While the CUI sector benefits from a highly skilled and competent workforce, individual infrastructure owners and operators cannot be expected to address national security risks on their own, without government intervention. Legislation is required to ensure damage to CUI is prevented as far as possible, and that standards for managing security and resilience risks are consistent and based on a clear understanding of the threat and hazards.
6. In recognition of these risks, the government has carried out a review of existing UK legislation to determine its effectiveness at addressing CUI security and resilience risks. It concluded that:
 - current legislation does not adequately deter harmful conduct affecting CUI;
 - security and resilience duties on the owners and operators of subsea telecoms cable infrastructure require strengthening;

- the government lacks sufficient powers to require action to address serious national security threats to subsea telecoms cable infrastructure; and
- current legislation does not provide an adequate framework for managing the national security risks associated with the deployment of new fibre-optic sensing technologies, or for enabling their potential benefits for infrastructure resilience to be realised.

7. This White Paper sets out proposals to introduce a new criminal penalties regime, new subsea telecoms infrastructure security and resilience duties and national security direction powers, and new fibre-optic sensing technology regulation.

Criminal penalties regime

8. The government proposes a new statutory framework to deter damage to, and interference with, critical undersea infrastructure. The framework would apply to subsea telecommunications cables, electricity interconnectors and pipelines, together with the infrastructure on which they depend.

9. The framework would create a new offence of causing a security compromise to critical undersea infrastructure, capturing both physical and non-physical interference, including remote electronic interference, cyber activity and certain preparatory conduct directed at compromising infrastructure. It would be supported by supplementary offences relating to matters such as obstructing repair operations and failing to preserve relevant evidence.

10. The government proposes a three-tier culpability structure distinguishing between intentional, reckless and grossly negligent conduct, with maximum penalties of up to 14 years' imprisonment for intentional conduct, 10 years for reckless conduct and two years for grossly negligent conduct, alongside unlimited fines. The government is also considering whether a higher maximum penalty should be available in the most serious cases.

11. The government is consulting on the territorial extent of the offences, including their application beyond the UK's territorial sea – for instance, where the offender is a UK national or where damage directly causes significant effects inside the UK. We are also consulting on whether further measures are needed to make it easier for infrastructure owners and operators to pursue civil claims to recover repair costs and other financial losses when CUI is damaged.

Security and resilience duties

12. It is important to ensure providers of subsea telecoms cable infrastructure are adopting appropriate and proportionate security and resilience measures. While the UK benefits from a highly capable and resilient cable sector, there are significant variations in the providers' risk management practices. Voluntary arrangements alone are not providing sufficient assurance of appropriate and proportionate security and resilience. The government's review has found that providers are not currently subject to consistent and enforceable security and resilience obligations.

13. The government therefore proposes new legislation to place security and resilience duties on providers of subsea telecoms infrastructure serving the UK.¹ Providers would be required to identify and mitigate risks to their infrastructure, prepare for and respond to security compromises, and recover as quickly as reasonably practicable following incidents.

¹ It would not apply to energy infrastructure, which is being considered as part of a separate process.

They would also be required to notify government and the appropriate regulator of security compromises and take reasonable and proportionate steps to inform directly affected users of significant risks.

14. We also propose creating new powers for the government to make secondary legislation and codes of practice setting out more detailed security and resilience requirements and technical guidance. This is intended to ensure that specific legal obligations can be updated to reflect changes in technology and the threat environment. A designated regulator would oversee compliance with this regulatory framework, supported by monitoring and enforcement powers and penalties aligned closely with existing legislation.

National security direction power

15. Government currently works closely with industry in responding to disruptive incidents. However, there may be circumstances in which urgent action is required from industry and voluntary cooperation alone cannot secure the response needed. The government's review identified a need for it to be able to compel industry to take specific actions to respond to serious national security incidents affecting subsea telecoms infrastructure when necessary. Existing legislation, notably Part 2 of the Civil Contingencies Act 2004, sets high thresholds for intervention and procedural steps that may be unworkable in responding to fast-moving subsea cable incidents.

16. The government therefore proposes creating a new power to enable the Secretary of State to direct providers of subsea telecoms infrastructure² and providers of subsea telecoms cable repair services, to take (or refrain from taking) specified actions in the interests of national security when necessary. The Secretary of State would need to be satisfied that a compromise of, or threat to, subsea telecoms infrastructure gives rise to a significant risk to national security and that the direction is necessary and proportionate in the interests of national security. The government expects the power would be used only exceptionally, as a measure of last resort. The government proposes that the power should be accompanied by appropriate safeguards ensuring that any intervention remains tightly constrained and proportionate to the risk being addressed.

Regulating sensing technology deployments

17. Sensing technologies deployed on subsea fibre-optic cables, including Distributed Acoustic Sensing (DAS), are capable of detecting changes in the surrounding marine environment. Such technologies offer significant benefits for hazard identification, infrastructure protection, and environmental research. However, they also pose a potential national security risk as they could generate data on sensitive defence assets that would be of interest to hostile actors. The government proposes a new statutory framework, consisting of a screening regime and baseline security requirements, to address this risk.

18. The screening regime would require those controlling the fibre on which sensing technologies are deployed to notify the government of current and future deployments. This would allow government to assess if they present a national security risk. Where needed, the government would impose bespoke conditions on a deployment or, in exceptional cases, prohibit it entirely where no other mitigation is sufficient.

19. Regardless of any bespoke conditions, controllers of the fibre on which sensing technologies are deployed would be subject to a set of baseline security requirements. These would be designed to protect the sensing technology deployments and the data

² Ibid.

they generate, as well as providing government access to the data where it is necessary and proportionate to do so. A designated regulator would oversee compliance with the requirements, supported by monitoring and enforcement powers and appropriate and proportionate penalties for non-compliance.

20. The government is also consulting on the territorial extent of the regime. It proposes that the regime should apply not only to sensing technology deployments on the UK end of cables landing in the UK, but also to deployments on cables passing through UK waters (including the exclusive economic zone), where such deployments are capable of detecting activity within those waters.

Next steps

21. The government is seeking views on these legislation proposals. Guidance on how to respond to the consultation (including an accompanying cost survey) is provided in Annex A. Specific consultation questions are set out throughout this White Paper and listed in full in Annex B. We will consider all the consultation responses and publish a formal government response to the feedback. We will also revise our proposals as necessary in response to the feedback we receive.

Chapter 1: Introduction

The infrastructure and why it matters

1.1 Thousands of cables, pipelines and interconnectors beneath our oceans and seas carry data and energy powering the global economy. Over the past 150 years we have become increasingly dependent on such critical undersea infrastructure (CUI), and our reliance upon it is likely to increase further in the coming decades. The infrastructure is built, owned, operated and maintained primarily by private sector companies.

1.2 Subsea telecoms cables are widely recognised as the backbone of the global internet. Cables the diameter of a garden hosepipe contain bundles of fibre-optic filaments conveying data via pulses of laser light. The world is connected by nearly 1.4 million kilometres of these cables, laid on the seabed in approximately 485 separate cable systems.³ Sixty-four active subsea telecoms cable systems land on UK shores. Forty-five of these are international cable systems, connecting us to other countries, and 19 are domestic cable systems, connecting the UK mainland to its islands offshore.

1.3 Subsea telecoms cables carry 99% of the UK's international data traffic. They provide access to the internet services upon which we depend. In doing so, they support all sectors of the UK economy, including finance, transport and government. Modern businesses depend on uninterrupted, high-capacity connectivity provided by such cables to operate effectively.

1.4 With increasing demands for data – due to AI, cloud computing and other digital applications – the UK's reliance on high-capacity international subsea cable connectivity is growing. Significant disruption to it could have immediate and cascading economic impacts, including interrupting financial flows, degrading business operations, and undermining investor confidence. Satellite systems can provide some resilience to disruption in certain circumstances but cannot replicate the capacity and speed of subsea systems.

1.5 The UK's energy supply also relies on a range of subsea infrastructure, and its economic significance should not be understated. Gas pipelines provide 74% of the UK's supply, while 10.3 gigawatts (GW) of installed electricity capacity comes from interconnector cables between the UK and Europe. These interconnectors and pipelines are a vital element of the UK's energy mix and system resilience, particularly during peak demand periods and times when both UK-based conventional and renewable output are low.

³ A subsea cable 'system' is the entire end-to-end network – including the physical cable, underwater signal repeaters and amplifiers, branching units, and land-based cable landing stations.

1.6 The UK's network of subsea energy infrastructure is steadily increasing, driven by growing UK energy demand and the energy transition. The Clean Power 2030 Action Plan targets 43-50 GW of offshore wind production (up from 14.8 GW currently), and over 20 GW of additional interconnector capacity. It is therefore critical that this infrastructure is adequately protected against a range of threats and hazards.

Security and resilience risks

1.7 Our subsea connectivity is highly resilient. Faults to CUI seldom result in significant disruption to end users of the services they provide. When faults on individual subsea telecoms cables occur data is diverted through alternative cables that carry spare capacity. Energy networks can be reconfigured to meet demand if there is disruption to subsea or offshore infrastructure. Industry has also developed sophisticated arrangements for repairing infrastructure when faults occur.

1.8 However, whilst subsea connectivity is resilient overall, much of the CUI remains vulnerable to disruption. This is demonstrated by the relatively large numbers of cable breaks occurring globally each year due to accidental dragging of anchors or fishing trawler nets across them. The concentration of data and energy conveyed through a relatively small number of critical assets contributes to potential service disruption risk.

1.9 Threats to CUI include potential physical sabotage and cyber-attacks, which could be carried out by proxies acting on behalf of others. In some cases, deliberate interference might be difficult to distinguish from accidental incidents, creating opportunities for hostile actors to obscure attribution and reinforcing the importance of maintaining effective deterrence, security and resilience.

1.10 Furthermore, the threat environment is changing. As the UK's National Security Strategy explains, the threats to the homeland from state actors are increasing and critical national infrastructure, including CUI, will continue to be a target.⁴ In April, the Defence Secretary John Healey revealed that our Armed Forces – in partnership with our allies – tracked Russian submarines whose mission was to survey cables. Such activity raises serious questions about the security and resilience of CUI globally, and the need for modern legal frameworks to protect it.

Rationale for legislation

1.11 Commercial incentives and voluntary arrangements alone will not ensure sufficient levels of security and resilience in response to the potential threats to CUI. Individual infrastructure owners and operators understandably focus on ensuring the continued availability of their own infrastructure and the services it provides to customers. However, they cannot be expected to address national security and resilience risks on their own, without government intervention. Legislation is required to provide deterrence and ensure consistent standards of CUI risk management, based on a clear understanding of the threats.

1.12 In its inquiry report on 'Subsea telecommunications cables: resilience and crisis management', the Parliamentary Joint Committee on the National Security Strategy (JCNSS) has been clear that UK legislation has failed to keep pace with the growing importance of CUI, or the risks it now faces.

⁴ *National Security Strategy 2025: Security for the British People in a Dangerous World (2025)*, p. 15, para. 10.

1.13 The government has undertaken a comprehensive review of domestic and international legislation to determine its effectiveness at addressing the risks to CUI and potential areas for improvement. It considered whether existing legislation remained fit for purpose in light of changing technologies, evolving threats and the growing strategic importance of subsea infrastructure to the UK. It was informed by engagement with regulators, external legal experts, international partners and industry stakeholders, including providers of subsea telecoms and energy infrastructure and representatives of the fishing sector.

1.14 The review examined the extent to which existing legislation deters harmful conduct, promotes appropriate levels of security and resilience, enables effective government intervention during serious incidents, and addresses the national security implications of sensing technologies. It also considered how the UK's legislation compares with that of international partners and how existing legislation interacts with wider regulatory, maritime and national security frameworks.

1.15 Our legislation review concluded that new criminal penalties, security and resilience duties, national security direction powers and sensing technology regulations are needed.

Structure of this White Paper

1.16 The chapters in this White Paper set out our legislation proposals in detail, inviting views from those with an interest in them, including CUI providers and maritime and fishing organisations:

- **Chapter 2: Key Terms** sets out the infrastructure, services and entities to which the proposals would apply under our legislation proposals. It explains the key definitions and concepts that underpin the proposals.
- **Chapter 3: Criminal Penalties Regime** sets out why the existing criminal penalties framework no longer provides an effective deterrent against harmful conduct affecting CUI. It proposes a modernised offence, stronger penalties and supporting enforcement measures designed to reflect the strategic importance of this infrastructure and the evolving threat environment.
- **Chapter 4: Security and Resilience Duties** sets out why providers of subsea telecoms infrastructure specifically should be subject to common security and resilience standards. It then proposes new duties to ensure security and resilience risks affecting this infrastructure are identified, managed and responded to consistently.
- **Chapter 5: National Security Direction Power** sets out why government needs additional powers to respond effectively to serious national security incidents affecting subsea telecoms infrastructure. It proposes a targeted power for the Secretary of State to require action when necessary and proportionate in the interests of national security.
- **Chapter 6: Regulation of Sensing Technologies** sets out the opportunities and national security risks arising from deployment of new sensing technologies on subsea fibre-optic cables. It proposes new legislation to ensure potential national security risks arising from the use of such technologies are managed appropriately.

1.17 The White Paper includes two annexes – **Annex A** which provides specific information on how to respond to the consultation (including an accompanying cost survey) and how the government plans to use the feedback and **Annex B** which contains a full list of the consultation questions.

Chapter 2: Key Terms

2.1 This chapter sets out the key terms and concepts that underpin the proposals within the White Paper.

Subsea conveyance systems and services

2.2 Critical undersea infrastructure (CUI) is the term used so far in this White Paper to refer collectively to subsea cables, pipelines and interconnectors. However, more precise terminology is required when considering how any new legislation will be applied. The following terms are therefore used in subsequent chapters:

- **Subsea data conveyance system** – defined as any subsea communications network conveying electronic signals, primarily through fibre-optic cables. This includes not only the cables, but also the supporting infrastructure on which the network depends to function, wherever located, such as the physical and digital components operating the cable (repeaters, branching units, power feed equipment, termination equipment, converter stations, substations and associated servers and control systems etc). It also includes the portion of the cable that runs onshore from landfall to its termination point on land.
- **Subsea data conveyance service** – defined as any service whose principal feature is the conveyance of signals provided by means of the subsea data conveyance system, or the provision of access to conveyance capacity for that purpose, by means of such a system.

Collectively, such systems and services are referred to in this White Paper as ‘**subsea data conveyance systems or services**’.

- **Subsea energy conveyance system** – defined as any subsea power cable, electricity or gas interconnector or pipeline, as well as any supporting infrastructure on which they depend to function (e.g. physical and digital components operating the cable, interconnector or pipeline) wherever located, including any above-surface offshore structures on which it depends, such as platforms. It also includes the portion of the cable, interconnector or pipeline that runs onshore from landfall to its termination point on land.
- **Subsea energy conveyance service** – defined as any service whose principal feature is the conveyance of energy provided by means of the subsea energy conveyance system, or the provision of access to conveyance capacity for that purpose, by means of such a system.

Collectively, such systems and services are referred to in this White Paper as **‘subsea energy conveyance systems or services’**.

The term **‘subsea conveyance systems or services’** is used to refer collectively to ‘subsea data conveyance systems or services’ and ‘subsea energy conveyance systems or services’.

Providers

2.3 The term **‘providers’** is used in this White Paper to refer to persons who own, operate or control such systems or services, as are referred to above. Where responsibility is shared across multiple parties, each party is considered a provider in relation to the element(s) it owns, operates or controls.

Security compromise

2.4 The term **‘security compromise’** is used within this White Paper to refer to:

- anything that compromises the availability, performance or functionality of the system or service;
- any unauthorised access to, or interference with, it; or
- any compromise of any data, signals, or energy it carries or generates.

2.5 This definition is intentionally broad. It captures physical damage and remote or electronic interference alike and applies to risks arising from natural hazards as well as human activity. It is not confined to any one sector, or to any particular means by which a compromise is brought about.

Consultation question

Q1. Do you agree with the proposed terms and definitions in this chapter? Please explain your answer.

Chapter 3: Criminal penalties regime

Background

3.1 The *Submarine Telegraph Act 1885* ('STA') remains the UK's principal piece of legislation designed specifically to protect subsea cables from harm. Its core rationale remains sound – that critical undersea infrastructure (CUI) warrants specific protection in criminal law, and that those responsible for damaging it should face the appropriate consequences.

3.2 However, the STA is now very outdated. It has not been updated to reflect technological advances, the growing importance of undersea infrastructure, or the evolving threat environment. The principal offence contained within the STA was drafted for a different era, focusing on protection of a now obsolete form of technology. It refers only to 'telegraphic' communications, creating uncertainty as to its application to modern fibre-optic cables, and it does not cover pipelines at all – despite them facing largely the same threats. Its application to power cables and electricity interconnectors remains untested. The penalties available under the Act also bear little relationship to the value of modern infrastructure or the cost of its repair. Responsibility for the STA's enforcement is also unclear.

3.3 The *National Security Act 2023* ('NSA') provides significant penalties – including life imprisonment – for sabotage, but only where foreign power involvement can be proven to the criminal standard. Where such involvement cannot be established, the available offences may be limited to the outdated provisions in the STA described above.

3.4 For these reasons, the government considers that new primary legislation is required to modernise and strengthen UK legislation to protect CUI and deter harmful conduct effectively.

Objectives

3.5 We consider the main objectives for the new primary legislation should be to:

- i) **Deter harmful conduct**, by establishing clear offences and penalties that reflect the seriousness and potential consequences of compromising subsea conveyance systems and services.
- ii) **Ensure the law can be effectively enforced** and offenders appropriately punished, through a modern and coherent framework that captures contemporary forms of harmful conduct and can be applied in practice.

- iii) **Avoid unnecessarily criminalising or constraining legitimate activity**, by ensuring that offences are clearly defined, proportionate and accompanied by appropriate safeguards and defences.

Consultation questions

Q2. *Do you agree that new primary legislation is required to modernise and strengthen UK legislation to protect CUI and deter harmful conduct effectively? Please explain your answer.*

Q3. *Do you agree with the proposed objectives for the criminal penalties regime? Please explain your answer.*

Overview of proposals

3.6 The government proposes to replace outdated provisions in the STA with a new statutory framework for deterring damage to, and interference with, subsea conveyance systems and services. The framework would create new modernised offences, strengthen penalties and liability, and ensure the offences are practically enforceable.

3.7 This chapter sets out our proposals for the new framework under the following headings:

- i) **Infrastructure in scope**
- ii) **New offences**
- iii) **Penalties and liability**
- iv) **Territorial extent**
- v) **Enforcement.**

Infrastructure in scope

3.8 The proposals in this chapter are intended to protect both subsea data and subsea energy conveyance systems and services, as defined in Chapter 2. Both face many of the same hazards and threats, and the consequences of their disruption can be comparably severe for the UK. The government therefore proposes a single criminal framework covering both sectors, ensuring that equivalent harmful conduct results in equivalent consequences for the perpetrators.

New offences

Core offence

3.9 The government proposes to introduce a core offence of conduct that causes a security compromise to a subsea conveyance system or service. 'Security compromise', as defined in Chapter 2, is intended to capture modern forms of hostile activity, such as remote electronic interference through cyber-attacks, as well as physical damage. A person would commit the offence where their conduct:

- results in a security compromise;
- is intended, planned or attempted to bring about a security compromise; or

- is likely to result in such a security compromise.

3.10 The proposed offence is intended to capture a person who maps, surveys or positions capability against infrastructure in preparation for a later attack, or who exploits it for covert surveillance, even where no loss of service has yet occurred. In defining the offence in this way, the government recognises that the legislation will need to be carefully designed so as not to inadvertently capture legitimate maritime, scientific and commercial operations.

3.11 The proposed offence is also intended to apply where the conduct is carried out through crewed, remotely operated or autonomous systems, so it covers technologies that are becoming increasingly accessible.

Supplementary offences

3.12 The government proposes including a set of supplementary offences to support deterrence and enforcement. These could include offences relating to:

- obstructing or significantly impeding repair operations;
- falsifying, destroying or failing to preserve relevant navigational, operational or vessel data; and
- failing to respond to lawful communications or directions from law enforcement bodies.

Consultation questions

Q4. Do you agree with the proposed approach to the offence framework? Please explain your answer.

Q5. Please let us know of any further views you have on the proposed offences.

Penalties and liability

3.13 It is important that in penalising the core offence set out above the framework recognises different levels of culpability. At present the STA criminalises only intentional and culpably negligent damage with the latter treated as a minor offence carrying very limited penalties. This approach risks under-penalising conduct that is unintentional but nonetheless reckless and conduct that is intentional but cannot be proven to the criminal standard (intent being notoriously difficult to prove where infrastructure is damaged at sea).

3.14 The government therefore proposes a three-tier culpability structure:

- **Intentional conduct** – deliberate conduct causing, or intended to cause, a security compromise;
- **Reckless conduct** – conscious disregard of a substantial risk of a security compromise; and
- **Grossly negligent conduct** – conduct falling far below expected standards and resulting in a security compromise or materially increasing its risk.

3.15 The government would not seek to define these concepts in primary legislation and would look to the courts to apply the well-established case law in this area.

3.16 The government proposes the following maximum penalties as proportionate to the potential harm and broadly in line with comparable legislation:

- **Up to 14 years' imprisonment for intentional conduct** – exceeding the Criminal Damage Act ('CDA') 1971 maximum, reflecting the potentially severe consequences of damage to subsea conveyance systems and services, but remaining below the life sentence for sabotage under the National Security Act 2023, which applies where conduct is linked to a foreign power and is therefore considered more serious;
- **Up to 10 years' imprisonment for reckless conduct** – in line with the CDA 1971 maximum, but lower than for intentional conduct so as not to over-penalise non-deliberate behaviour;
- **Up to two years' imprisonment for grossly negligent conduct** – a substantially lower maximum for conduct that falls below the expected standards of behaviour without meeting the threshold of recklessness. This maximum is consistent with navigational offences under the Merchant Shipping Act ('MSA') 1995 but remains a significant increase on the current three-month maximum under the STA 1885;
- **Up to two years' imprisonment for the supplementary offences** – aligned with the proposed penalty for grossly negligent damage and with existing penalties for navigational offences under the MSA 1995; and
- **Unlimited fines across all categories, including for legal persons** – giving courts flexibility to reflect the scale and resources of corporate offenders, and providing a meaningful deterrent for individual offenders.

3.17 The government is also considering whether a higher maximum penalty, including life imprisonment, should be available where intentional or reckless conduct causes, or risks causing, loss of life or serious prejudice to national security or other essential interests. The aim would be to ensure courts have greater flexibility in cases with catastrophic consequences.

Liability of legal persons

3.18 The government proposes that the offence framework should apply to legal persons, as well as individuals. This might occur where a security compromise results from:

- corporate policy, decision-making or direction;
- failures of oversight, systems or procedures; or
- acts or omissions of employees or agents acting within the scope of their role, where fault can properly be attributed to the organisation.

Defences

3.19 The government proposes a set of clear statutory defences to ensure that legitimate and responsible action, taken in good faith, is not criminalised or discouraged. Such defences would apply only where all necessary precautions had been taken and would be carefully designed so as not to protect deliberate, reckless or grossly negligent behaviour. The defences could include:

- actions taken to save life;
- actions taken to preserve a vessel;

- inadvertent damage occurring in the course of repair or maintenance of submarine infrastructure;
- actions taken under duress; and
- actions taken in compliance with a legal obligation under UK law that is not a legal obligation under private law.

Consultation questions

Q6. Do you agree with the proposed approach to penalties and liability? Please explain your answer, including any views on proportionality and deterrence.

Q7. Please let us know of any further views you have on the proposed penalties.

Territorial extent

3.20 The territorial extent of the offences is important to define as much of the infrastructure the framework is designed to protect lies beyond UK territory. The UK's territorial sea extends up to 12 nautical miles from the coast, and within it the UK exercises full jurisdiction. Beyond that lies the exclusive economic zone (EEZ), which extends up to 200 nautical miles from the coast. Within this zone the UK exercises exclusive rights to the natural resources but has otherwise more limited jurisdiction. Beyond this is either the high seas or EEZs of other coastal states. Generally, UK criminal law does not apply to conduct beyond UK territory, except in certain circumstances – for instance where the offender is a UK national, or where the conduct directly causes significant effects within UK territory.

3.21 The government proposes that the offences should apply where:

- the conduct occurs within the UK's territory or territorial sea, regardless of an individual's nationality or a vessel's flag state;
- the conduct is carried out by a UK national or a UK-flagged vessel operating in international waters; or
- the conduct occurs beyond the UK's territorial sea, affects infrastructure connecting to the UK, and is likely to have significant effects within the UK.

3.22 This proposed extraterritorial jurisdiction reflects the reality that damage to subsea conveyance systems commonly occurs beyond the territorial sea. Confining the offences exclusively to UK territory would put large sections of the infrastructure the UK relies upon entirely beyond the reach of its criminal law. The government considers this approach justifiable under international law but recognises state practice in this area is not settled and is therefore seeking views through this consultation on the proposed approach.

Devolution and Crown Dependencies

3.23 While the proposals in this chapter are driven by reserved competences – principally national security, defence and telecommunications – the UK government recognises that they also touch upon areas of devolved competence, specifically aspects of criminal justice in Scotland and Northern Ireland. We have engaged officials in the devolved governments in the development of this White Paper. If the proposals progress beyond consultation, we will work closely with them in developing the legislation to ensure an aligned approach across the whole of the United Kingdom.

3.24 The government also recognises the importance of a consistent approach with the Crown Dependencies. In developing any future legislation we will work with them to ensure an aligned approach to the protection of this critical infrastructure.

Consultation question

Q8. Do you agree with the proposed territorial extent? Please explain your answer.

Enforcement

Enforcement powers

3.25 The government intends to set out enforcement powers explicitly in primary legislation. Where an offence occurs on land, the ordinary powers of investigation, arrest and prosecution would apply. Where conduct occurs at sea, the offences would be supported by maritime enforcement powers to stop, board, divert and detain a vessel, require compliance from its master or crew, require a vessel to be taken to port, and to preserve evidence. This would also include powers exercisable against foreign-flagged vessels in accordance with international law. The government does not propose a separate enforcement regime but rather to mirror existing legislation.

Civil remedies

3.26 Damage to subsea infrastructure can impose significant costs on operators, including repair costs, lost revenue and service disruption. Operators seeking to recover those losses through the civil courts often face practical and evidential difficulties, including attributing fault, securing evidence from the seabed, and identifying those responsible in a timely manner.

3.27 The government considers that the new framework should support infrastructure owners and operators in recovering repair costs and other financial losses resulting from conduct it is designed to prevent. Section 105W of the Communications Act 2003 (inserted by the Telecommunications (Security) Act 2021) makes the breach of specified duties in that Act directly actionable in civil proceedings by a person who suffers loss or damage. A similar provision could give claimants a clearer statutory basis for claims arising from conduct that constitutes an offence under the proposed legislation in this chapter, rather than relying on less direct routes to establish liability.

3.28 **The government is seeking views on whether such a provision should be included, and if any further measures might also support the fair and effective recovery of repair costs and other financial losses through the civil courts.** For example, we are considering whether improved access to navigational, vessel-tracking and other evidential data could assist claimants in establishing responsibility for damage, or whether the law should make it easier to establish liability in clearly defined circumstances. Any measure would need to be balanced and carefully designed so as not to place disproportionate burdens on legitimate maritime activity, particularly the fishing and merchant shipping sectors, and so as not to predetermine liability in individual cases.

3.29 This proposal sits alongside the new security and resilience duties set out in Chapter 4. Together, they are intended to ensure that responsibility for protecting this infrastructure is shared appropriately between those who own and operate it and those whose activities could cause damage to it.

Consultation questions

Q9. Do you agree with the proposed approach to enforcement? Please explain your answer.

Q10. Do you think any changes to existing enforcement powers are required to give practical effect to the proposed offences? Please explain your answer.

Q11. Please let us know of any further views you have on enforcement.

Chapter 4: Security and Resilience Duties

Background

4.1 Providers of subsea data conveyance systems and services are not currently subject to consistent legal requirements to take appropriate and proportionate measures to protect them against security threats.

4.2 Providers have strong commercial incentives to maintain the availability of their services, and the sector invests accordingly. However, those incentives do not consistently extend to the measures needed to address sophisticated security threats, or to ensure preparedness for high-impact, low-likelihood scenarios in which several cable systems are compromised at once.

4.3 Practice varies across the sector in how risks of security compromise are identified and assessed, how physical and digital assets are protected, and how providers prepare for, and coordinate, their response to incidents. The government considers that this leaves significant inconsistencies and gaps in baseline protection, preparedness and incident coordination across the sector.

4.4 Existing legislation does not establish consistent and enforceable security and resilience duties across all providers of subsea data conveyance systems or services. The Telecommunications (Security) Act 2021 amended the Communications Act 2003 to establish new security and resilience duties for the providers of public electronic communications networks or services (PECN or PECS) in the UK. However, not all subsea data conveyance systems or services are within scope of this legislation. Some relevant systems and services are directly regulated, some are captured only indirectly, and others may fall outside the existing framework. Other legislation, including marine licensing under the Marine and Coastal Access Act 2009 and the Marine (Scotland) Act 2010, regulates activity on the seabed rather than infrastructure security and resilience.

4.5 **For these reasons, the government proposes to introduce new duties in primary legislation on providers of subsea data conveyance systems and services to establish clear and consistent security and resilience standards.**

Objectives

4.6 We consider the main objectives for new primary legislation should be to ensure:

- i) **Our national security is strengthened through all relevant providers taking appropriate and proportionate measures to identify and mitigate security and resilience risks to their infrastructure.**
- ii) **Relevant providers are able to anticipate, detect and respond to subsea cable incidents effectively**, including malicious interference and complex disruption scenarios, through improved baseline security practices, resilience planning and cooperation with government.
- iii) **Security and resilience risks are managed consistently across cable systems**, including where infrastructure is located in the territorial sea or beyond, through clear and enforceable obligations that support timely remediation and coordinated incident response.
- iv) **Regulatory clarity and consistency are improved**, by resolving ambiguities in how security and resilience duties apply to subsea systems and services.

Consultation questions

Q12. Do you agree that new duties in primary legislation on providers of subsea data conveyance systems and services are required to establish clear and consistent security and resilience standards? Please explain your answer.

Q13. Do you agree with the proposed objectives for the security and resilience duties? Please explain your answer.

Overview of proposals

4.7 The government proposes to introduce a new legislative framework placing clear, enforceable security and resilience duties on the providers of subsea data conveyance systems or services. These duties would build on existing measures within the Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021), which are designed to ensure the security and resilience of UK public telecoms networks and services. The duties would be supported by more specific regulations set out in secondary legislation and codes of practice providing technical guidance on compliance.

4.8 This chapter sets out our proposals under the following headings:

- i) **Duties on providers**
- ii) **Secondary legislation and codes of practice**
- iii) **Entities, systems and services in scope**
- iv) **Territorial extent**
- v) **Monitoring and enforcement.**

Duties on providers

4.9 The government proposes placing a number of duties on providers of subsea data conveyance systems or services to improve the security and resilience of this critical infrastructure. These duties are intended to establish a risk-based framework that supports the prevention, detection and management of security compromises, strengthens government and regulatory oversight, and promotes effective coordination and information sharing when incidents occur. The proposed duties are outlined below.

Duty to take appropriate and proportionate measures to manage the risk of security compromise

4.10 The first duty would be for providers to take appropriate and proportionate measures to manage the risk of security compromises occurring. This would include obligations to identify and assess security compromise risks, reduce vulnerabilities, and prepare for potential incidents. This is intended to ensure that providers take a comprehensive, risk-based approach to the security and resilience of the systems and services they operate.

4.11 In this context, a 'security compromise' would draw on the existing statutory definition set out in the Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021), ensuring consistency with the UK's wider telecommunications security framework. The definition is intentionally broad, capturing a range of risks including: loss of availability, performance or functionality; unauthorised access or interference; and the compromise of data or signals. This approach would ensure that the framework is effective at addressing both physical and non-physical risks, including those arising from natural hazards, accidental damage and malicious activity.

Duty to take measures in response to security compromises

4.12 The second duty would be for providers to take appropriate and proportionate measures in response to security compromises. This would include obligations to respond to, mitigate and recover from security compromises where they occur, and to take steps to minimise their impact on the systems and services they operate. This is intended to ensure that providers are able to act effectively when incidents arise, limiting disruption and restoring normal operations as quickly as reasonably practicable.

Duty to notify government and the appropriate regulator of any security compromise

4.13 The third duty would be for providers to notify government and the appropriate regulator of any security compromise affecting subsea data conveyance systems or services, including cable faults and outages, as soon as reasonably practicable. Timely reporting supports improved situational awareness, enables more effective coordination of responses to incidents, and helps strengthen the UK's overall resilience to disruption.

Duty to inform others of significant risk of security compromise

4.14 The fourth duty would be for providers to take reasonable and proportionate steps to inform users of significant risks of security compromise. Where there is a significant risk of a security compromise occurring, providers would be required to take reasonable and proportionate steps to bring relevant information to the attention of subsea data conveyance system or service users who may be adversely affected. The duty would extend only to direct users (i.e. those entities the provider directly engages with).

4.15 The duty would include sharing information about the nature of the risk, any measures that users could reasonably take to prevent, mitigate or remedy adverse effects, and details of a point of contact for further information. This is intended to ensure that users are

appropriately informed about significant security risks, enabling them to take practical steps to protect themselves and reducing the potential impact of security compromises where they occur.

4.16 By “reasonable and proportionate”, we mean that providers should provide information that is sufficient to enable affected users to understand the nature and potential impact of the risk and to take appropriate mitigating action. This duty is not intended to require providers to disclose sensitive operational details, security vulnerabilities, or other information where disclosure could itself increase security risks. Rather, providers should balance the need to inform users with the need to protect the security of the subsea data conveyance system or service, while also identifying where these two things mutually reinforce one another.

Duty to register

4.17 The government is seeking views on whether the framework should include an additional duty requiring providers of subsea data conveyance systems or services to register with the designated regulator. A registration requirement would support the effective operation of the framework by ensuring that government and the regulator have a clear and up-to-date understanding of the infrastructure, services and providers within scope. The ownership and operation of subsea infrastructure can be complex, involving consortium arrangements, infrastructure investors, capacity providers and operators with different responsibilities across the cable system. Without a registration requirement, it may be difficult to identify all entities subject to the framework, assess the extent of critical infrastructure connected to the UK, and ensure that regulatory obligations are being applied consistently.

4.18 Registration could require providers to supply information about the infrastructure and services they own, operate or control, together with relevant information about ownership, operational responsibilities and points of contact. This would support supervisory activity, facilitate engagement during incidents, improve government and the regulator’s understanding of the sector, and help ensure that security and resilience duties are applied effectively across the whole subsea cable ecosystem.

4.19 The government is interested in views on whether a registration requirement is necessary, what information should be provided, how frequently it should be updated, and whether any categories of provider or infrastructure should be excluded from the requirement.

Consultation questions

Q14. Do you agree with the proposal to introduce the following security and resilience duties:

- *Duty to take appropriate and proportionate measures to manage the risk of security compromise*
- *Duty to take measures in response to security compromises*
- *Duty to notify government and the appropriate regulator of any security compromise*
- *Duty to inform others of significant risk of security compromise?*

Please explain your answer.

Q15. What are your views on whether a registration requirement should be introduced for the providers of subsea data conveyance systems or services?

Q16. Please let us know of any further views you have on the proposed duties, including if you think anything is missing.

Secondary legislation and codes of practice

Power for the government to make regulations

4.20 In addition to obligations on providers set out in primary legislation, the government proposes that it should be able to set detailed requirements through regulations, requiring providers of subsea data conveyance systems or services to take specific measures. The proposed duties described in the previous paragraphs are deliberately high-level so that they remain relevant as threats, technologies and ownership models change. On their own, however, they would leave providers uncertain about what compliance actually requires, and the regulator without a firm basis on which to enforce. Existing legislation, such as the Telecommunications (Security) Act 2021, resolves this by combining broad duties in primary legislation with specific regulatory requirements in secondary legislation and technical guidance in codes of practice. This layered approach means requirements can be updated as risks evolve, without needing new primary legislation each time. We propose a similar approach, providing the government with the power to make new regulations in secondary legislation setting out specific measures required of providers to meet each of the high-level duties set out in primary legislation.

Powers for the government to make codes of practice

4.21 The government proposes that it should be able to issue codes of practice to provide detailed technical guidance for providers on how to comply with the duties in primary legislation and requirements set out in the regulations.

Consultation questions

Q17. Do you agree that detailed security and resilience requirements should be set out in regulations within secondary legislation? Please explain your answer.

Q18. Do you agree that government should be able to issue codes of practice providing guidance on how providers can comply with their duties and regulatory requirements? Please explain your answer.

Q19. Please let us know of any further views you have on the proposed use of secondary legislation and codes of practice.

Entities, systems and services in scope

4.22 The ownership and operation of subsea data conveyance systems and services is often complex and distributed across multiple parties. Individual cable systems are frequently developed, financed and operated through consortium arrangements involving a range of entities with differing roles, rights and responsibilities, including infrastructure owners, capacity providers and service operators. Different parts of a cable system, such as subsea segments, landing stations and associated onshore infrastructure, may be owned or operated by different actors across different jurisdictions.

4.23 Investment patterns in the systems are evolving. In addition to traditional telecommunications operators, a wider range of entities are now investing in and developing them, including hyperscale technology companies and financial investors. These developments are increasing the scale and pace of deployment but also introducing more

complex ownership structures and operational models. This complexity reinforces the need for a framework that applies consistently to those who own or control subsea data conveyance systems and services.

Entities in scope

4.24 The government proposes that the duties in primary legislation should apply to the providers of subsea data conveyance systems or services, as defined in Chapter 2.⁵ Where responsibility is shared across multiple parties, each party is considered a provider in relation to the element(s) it owns, operates or controls. The intention is that the regime will apply to legal persons that are responsible for subsea data conveyance systems or services, not the downstream connectivity services that use subsea routes incidentally.

4.25 Where a system or service is provided by a consortium of companies, the government proposes that all members of the consortium should be subject to an individual legal obligation. The government further proposes that the regime should allow the relevant regulator to require designation of a lead entity for engagement, reporting, notifications and coordination. Designating a lead should not absolve other consortium members of their underlying legal duties. The designated regulator should be able to direct information requests or requirements to either the lead or individual members where necessary.

Systems and services in scope

4.26 Providers would be required to comply with the proposed security and resilience duties in relation to the subsea data conveyance systems or services they own, operate or control. This means providers would be responsible for taking appropriate and proportionate measures in relation to the parts of the system or service they are responsible for, including where responsibility is shared across multiple parties. The broad definitions of subsea data conveyance systems and services in Chapter 2 are intended to help ensure the duties can be applied effectively to the broad range of systems and services requiring protection.

4.27 The government does not intend for the duties to apply to systems or services whose sole purpose is to provide connectivity to offshore infrastructure, installations or facilities. This exclusion would apply to cables that do not provide, support or form part of a subsea data conveyance system or service connected to the wider provision of electronic communications services within, to or from the United Kingdom. This includes, for example, cables used exclusively to support the operation, monitoring or control of offshore energy installations or other offshore industrial assets. The government considers that the security and resilience risks associated with such infrastructure would be more appropriately addressed through other sector-specific regulatory frameworks.

Avoidance of dual regulation

4.28 We propose including provisions to avoid providers being subject to both the new duties and existing security and resilience duties in the Communications Act 2003 for the subsea data conveyance systems and services they provide. We wish to avoid

⁵ Providers of subsea energy conveyance systems or services would not be within scope of these specific duties. Subsea data and energy infrastructure have distinct technical characteristics, which require bespoke security and resilience requirements. The government is considering physical resilience measures for the whole of the energy network, including onshore and offshore systems, separately, to a different timeframe.

dual regulation. Our intention is that the duties proposed in this chapter and the existing duties in the Communications Act (as amended by the Telecommunications (Security) Act 2021) should complement one another.

Consultation questions

Q20. Do you agree with the proposed approach to the providers in scope of the security and resilience duties? Please explain your answer.

Q21. Do you agree with the proposed approach to the systems and services in scope of the security and resilience duties? Please explain your answer.

Q22. Do you agree with the proposed approach for avoiding dual regulation? Please explain your answer.

Q23. Please let us know of any further views you have on the scope of the duties.

Territorial extent

4.29 The duties we are proposing would apply consistently across the whole of the United Kingdom. Telecommunications and national security are reserved matters, and the duties would therefore extend to England and Wales, Scotland and Northern Ireland on the same basis.

4.30 The government proposes that the duties should expressly extend to the UK's territorial sea. Damage to the systems and services within the territorial sea can have very similar consequences to damage on land (i.e. loss of the communications services). Ensuring the duties apply to the territorial sea would allow obligations to apply within a particularly high-risk zone for subsea cables. Cable density is highest in the territorial sea, cables converge towards landing stations, and human activity is at its most intense. The UK exercises full sovereignty within its territorial sea, and existing regulatory regimes already apply within it (e.g. the Marine and Coastal Access Act 2009 (MCAA) and the Marine (Scotland) Act 2010 in Scotland).

Consultation questions

Q24. Do you agree that the duties should apply within the UK's territorial sea? Please explain your answer.

Q25. Please let us know of any further views you have on the proposed territorial extent of the security and resilience duties.

Monitoring and enforcement

4.31 The government proposes that a designated regulator should have a set of powers to monitor and enforce providers' compliance with the duties, consistent with existing powers under the Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021). The regulator's monitoring and enforcement powers would include, but not be limited to:

- i) The power to assess compliance with security and resilience duties and regulations applicable to providers of subsea data conveyance systems or services,

- ii) The power to give assessment notices in respect of the providers' compliance with the security duties and regulations, and
- iii) The power to enforce penalties where non-compliance with the security duties and regulations occurs.

4.32 The government proposes that the designated regulator should be able to issue financial penalties to providers for non-compliance with the duties of up to £10 million or 10% of a provider's qualifying worldwide revenue, whichever is higher. The government also proposes that the designated regulator should have powers to impose continuing penalties where contraventions persist. These penalties are intended to reflect the seriousness of non-compliance, and potential harm it could cause.

Consultation questions

Q26. Do you agree with the proposed monitoring and enforcement powers? Please explain your answer.

Q27. Are there any additional monitoring or enforcement powers that should be available to the regulator? Please explain your answer.

Q28. Please let us know of any further views you have on the proposed monitoring and enforcement proposals.

Chapter 5: National Security

Direction Power

Background

5.1 The security and resilience duties set out in the previous chapter will help to establish a set of baseline standards across the sector. However, there may be unforeseen circumstances in which government needs to intervene to address acute national security risks, such as those arising from a major national security incident.

5.2 In such circumstances, the government needs the ability to compel industry to take urgent action to prevent, mitigate or otherwise respond to a serious incident. This may include gathering information relating to a suspected compromise, providing access to the infrastructure or implementing temporary security measures.

5.3 Whilst government may advise and recommend such actions, there is currently no clear statutory basis on which providers of subsea data conveyance systems or services can be compelled to act. Existing legislation, notably Part 2 of the Civil Contingencies Act 2004, sets a high threshold for intervention and involves procedural steps that may not be workable in fast-moving subsea cable incidents.

5.4 Powers of this kind are already well established in other critical sectors, for example in the water sector under the Water Industry Act 1991, and in air traffic services under the Transport Act 2000. A similar national security direction power has been included in the Cyber Security and Resilience Bill currently before Parliament.

5.5 **For these reasons, the government considers that new primary legislation is required to enable the government to compel action in specific circumstances in the interests of national security.**

Objectives

5.6 We consider the main objectives for new primary legislation should be to ensure:

- i) **Specific actions are rapidly taken by industry** in response to serious national security threats or major incidents affecting the UK's subsea cable connectivity.
- ii) **Government has the flexibility to define precisely what action is required** in response to any serious national security threat or incident.

Consultation questions

Q29. Do you agree that new primary legislation is required to enable the government to compel action in specific circumstances in the interests of national security? Please explain your answer.

Q30. Do you agree with the proposed objectives of the national security direction power? Please explain your answer.

Overview of proposals

5.7 The government proposes to create a new direction power in primary legislation enabling the Secretary of State to require specified action where this is necessary and proportionate in the interests of national security. The power would apply only where cooperation through existing regulatory frameworks or voluntary action cannot reasonably be relied upon to deliver the response required. It is intended to operate as a tightly constrained backstop, rather than as a substitute for normal operational decision-making.

5.8 This chapter sets out our proposals under the following headings:

- i) **Entities in scope**
- ii) **Direction power**
- iii) **Territorial extent**
- iv) **Monitoring and enforcement.**

Entities in scope

5.9 The government proposes that directions issued by the Secretary of State using the power should be able to apply to:

- **providers of subsea data conveyance systems or services**, as defined in Chapter 2; and
- **providers of subsea data conveyance system or service repair capabilities**, including providers of vessels and equipment capable of being used for the installation, repair, maintenance or recovery of subsea data conveyance systems or services.

5.10 We do not propose including providers of subsea energy conveyance systems or services within scope. The government is considering separately to this proposed legislation whether similar national security direction powers are necessary for energy.

5.11 To ensure the framework remains effective as the sector evolves, the government proposes that the Secretary of State should be able to bring additional categories of entities within scope through secondary legislation, where the security and resilience of subsea cable connectivity depend on them. Such secondary legislation would be subject to consultation and to the affirmative procedure.

Consultation questions

Q31. Do you agree with the proposed entities in scope? Are there other entities that should be within scope? Please explain your answer.

Q32. Please let us know of any further views you have on the entities in scope of the power.

Direction power

When the power might be used

5.12 The government proposes the Secretary of State should be able to direct entities within scope to take or refrain from taking specified action only when the Secretary of State is satisfied that:

- a compromise of, or a threat to, a subsea data conveyance system or service gives rise to a risk to national security; and
- the issuing of the direction is necessary and proportionate in the interests of national security.

5.13 The threshold is deliberately high. It requires a specific compromise or threat, rather than general concerns about the security of the sector. The government expects the power to be used only in exceptional circumstances and as a backstop where existing commercial arrangements, regulation or voluntary action cannot reasonably be relied upon to deliver the response required.

5.14 The government does not consider it appropriate to define exhaustively the circumstances in which a direction may be given. Examples could include a credible intelligence warning relating to subsea infrastructure, a serious security compromise affecting one or more cable systems, a risk of widespread disruption to UK connectivity arising from a natural hazard, or other circumstances in which government assesses that urgent action is required to protect national security or the continued provision of subsea data conveyance services.

Requirements a direction could impose

5.15 The government proposes that directions issued by the Secretary of State using the power should require the providers referred to above to take specified actions in relation to the security and resilience of subsea data conveyance systems or services, as defined in Chapter 2.

5.16 Indicative examples of the types of requirements a direction might include are:

Information gathering requirements to:

- provide information to the government in connection with a specific threat or incident, for instance regarding system capacity, routing, traffic flows, service impacts, the status of a fault or repair;
- enable access by specific public bodies to cable landing stations and related sites to assess vulnerabilities.

Incident prevention requirements to:

- cooperate with the implementation of temporary security measures at sites assessed to face a heightened national security risk;
- prohibit or restrict the use, installation or operation of specified goods, services or facilities, and requirements to remove, disable or modify specified goods or facilities, or to modify services.

Incident investigation requirements to:

- survey or inspect a cable, landing station or associated infrastructure to identify evidence of interference or compromise;
- preserve records, data or physical evidence relevant to an incident;
- delay remedial or repair activity, where immediate action would prejudice investigation or attribution.

Impact management requirements to:

- ensure temporary reconfiguration or rerouting of traffic, isolation of affected systems, or prioritisation of connectivity supporting essential services.

Incident remediation requirements to:

- ensure incident response is prioritised appropriately based on national interest, including the prioritisation of repairs where continued disruption would have the most serious national impacts.

Supporting requirements to:

- appoint a suitably qualified person, subject to the Secretary of State's approval, to assist in complying with the direction.

5.17 In exercising the power, the government would have regard to what is reasonably practicable in the circumstances, including operational, technical and safety constraints. The government recognises that directions may need to be implemented in conditions of significant uncertainty and that the availability of vessels, equipment, personnel and access may be constrained during a major incident.

Safeguards

5.18 The government is clear that a broad power of this kind must be accompanied by robust safeguards. Therefore, we propose that:

- a direction can only require actions in relation to the security and resilience of subsea data conveyance systems and services;
- a direction must specify the reasons for it, except where, and to the extent that, the Secretary of State considers that setting out those reasons would be contrary to the interests of national security;
- before giving a direction, the Secretary of State must consult the entity to be directed, and such other entities as appropriate, so far as reasonably practicable having regard to the urgency of the circumstances, except where to do so would be contrary to the interests of national security;
- the Secretary of State must keep directions under review and may vary or revoke them, giving notice of any variation or revocation;

- once a direction has been given, the Secretary of State must lay a copy of it (and any variation) before Parliament, subject to exclusions where publication would be contrary to national security or would unreasonably harm commercial interests;
- a direction, and its contents, may be made subject to a non-disclosure requirement where the Secretary of State considers this necessary and proportionate in the interests of national security;
- a direction must specify when it comes into force and, for any requirement to take action, a reasonable period within which that action must be taken; and
- any variation of a direction must itself meet the threshold for giving a direction, so that a direction cannot be broadened without a fresh assessment that doing so is necessary and proportionate in the interests of national security.

Interaction with other regimes

5.19 In some cases, action taken under a direction could potentially conflict with obligations under existing regulatory regimes (e.g. licence conditions under the Marine and Coastal Access Act 2009). It could also interact with the proposed security and resilience duties, including those relating to incident reporting and customer notification.

5.20 The government proposes that compliance with a direction should generally take precedence over other requirements in legislation, provided such compliance is compatible with the government's international law obligations. The government will ensure the framework makes appropriate provision for how such interactions are managed, so that directed entities can act quickly where necessary without being left in breach of other legal obligations, while ensuring relevant regulators are informed where a requirement they enforce is affected.

Information gathering and sharing

5.21 The government proposes that the Secretary of State would have a standing power to require information from entities in scope. This would help the government maintain an accurate understanding of the sector over time (including infrastructure, capacity and repair capability), so that it is well placed to identify risks and, if a direction becomes necessary, to design it effectively. This power would ordinarily be used by the government to help it prepare for incidents, rather than during incident response. Where information is needed urgently in response to a specific threat or incident, it could also be required through a national security direction, as set out above. The power would be subject to appropriate limits, including protection for legally privileged material.

5.22 The Secretary of State would be able to share information obtained through the use of this power with relevant public authorities, where necessary and proportionate in the interests of national security. This reflects the need for close coordination between public authorities in response to major incidents. Any such information sharing would be limited to what is relevant and proportionate to the purpose for which it is made.

Consultation questions

Q33. Do you agree with the proposed threshold for exercising the direction power, namely that the Secretary of State must be satisfied that a compromise of, or threat to, a subsea data conveyance system or service gives rise to a risk to national security? Please explain your answer.

Q34. Do you agree with the types of requirements a direction could impose that we have proposed? Please explain your answer.

Q35. Do you agree with the proposed safeguards on the exercise of the direction power? Are any additional safeguards needed? Please explain your answer.

Q36. Do you agree with the proposal that compliance with a direction should generally take precedence over other requirements in legislation, provided such compliance is compatible with the government's international law obligations? Please explain your answer.

Q37. Do you agree with the proposed standing power for the Secretary of State to require information from entities in scope to help the government maintain an accurate understanding of the sector? Please explain your answer.

Q38. Please let us know of any further views you have on the direction power itself.

Territorial extent

5.23 The government expects the proposed direction power to apply consistently across the whole of the United Kingdom. Telecommunications and national security are reserved matters, and the power would therefore extend to England and Wales, Scotland and Northern Ireland on that basis.

5.24 The national security direction proposals would cover subsea data conveyance systems and services as defined in Chapter 2 that are connected to the UK. **We propose that a direction may have effect along the full extent of the system or service, including beyond the UK's territorial sea, where the national security risk or impact arises in relation to the UK.**

5.25 In relation to providers of subsea data conveyance system or service repair capabilities, a direction may have effect whether the capability is located in the UK or its territorial sea, or elsewhere where there is a sufficient connection to the UK to bring the capability (e.g. vessel or equipment) within UK jurisdiction.

5.26 Where a direction would require action outside the UK's territorial sea, the power would be exercised consistently with international law and, where necessary, in cooperation with other states (see 'International coordination' section below).

5.27 The government intends to work with the Crown Dependencies and relevant Overseas Territories to ensure an aligned approach.

International coordination

5.28 The government recognises that subsea cables are, by their nature, shared international infrastructure, and that action taken under these powers may have implications for other states. The government will ensure that the exercise of these powers is consistent

with the UK's international legal obligations and coordinated, where appropriate, with international partners who share an interest in the affected infrastructure. The government is also considering how these powers align with other states' equivalent legal mechanisms.

Consultation questions

Q39. Do you agree with the proposed territorial extent of the power, including that a direction may have effect beyond the UK's territorial sea? Please explain your answer.

Q40. Do you agree with the proposal that a direction may have effect along the full extent of the system or service, including beyond the UK's territorial sea, where the national security risk or impact arises in relation to the UK? Please explain your answer.

Q41. Do you have views on how use of the power should be coordinated with other states that share subsea systems connecting to the UK? Please explain your answer.

Q42. Please let us know of any further views you have on the proposed territorial extent of the power.

Monitoring and enforcement

5.29 Compliance with the directions would be monitored and enforced by central government, reflecting the national security basis for their use. **To support this, we propose specific powers for the government to require information relating to compliance with a direction and, where necessary, to carry out or require inspections.** Any inspection powers would be subject to appropriate limits, including notice requirements, protection for legally privileged material and safeguards on entry to premises.

5.30 Where an entity contravenes a direction or a related requirement, the Secretary of State would be able to issue a notification setting out the contravention and the steps required to remedy it, followed where necessary by a confirmation decision requiring the entity to take specified action within a specified period. A confirmation decision may also require the payment of a financial penalty.

5.31 Any penalty would have to be appropriate and proportionate to the contravention in respect of which it is imposed. **The government proposes the following maximum penalties for non-compliance:**

- for contraventions of a national security direction, up to £17 million or 10% of global turnover (whichever is higher), with daily penalties of up to £100,000 for continuing contraventions;
- for failures to comply with information-gathering or inspection requirements, up to £10 million, with daily penalties of up to £50,000; and
- for contraventions of a non-disclosure requirement, the same maximum amounts as apply to the information-gathering and inspection requirements.

5.32 **The government also proposes that the Secretary of State should be able to amend these amounts through secondary legislation to reflect inflation.**

Consultation questions

Q43. Do you agree with the proposed approach to monitoring and enforcement? Please explain your answer.

Q44. Do you think the proposed financial penalties are appropriate and proportionate? Please explain your answer.

Q45. Please let us know of any further views you have on monitoring and enforcement of compliance with the directions that would be issued under the proposed power.

Chapter 6: Regulation of Sensing Technologies

Background

6.1 Recent technological developments have made it possible to use the optical fibres inside subsea cables to detect activity around them. Known collectively as fibre-optic sensing, these technologies turn the cable itself into a sensor, capable of detecting vibration or temperature changes along its length. Examples of such sensing technologies include Distributed Acoustic Sensing (DAS) and Distributed Temperature Sensing (DTS). They can be used to monitor the condition of the infrastructure itself, detect environmental changes, seismic activity or nearby vessel traffic, as well as locate faults or interference. The technology is advancing rapidly, and it is likely that more detailed and accurate data will be collected and processed through the use of fibre-optic sensing in the near future.

6.2 This creates significant opportunities. Continuous monitoring can give operators early warning of hazards such as anchor drags or seabed disturbance, allowing faster intervention and reduced outage times. The same data can support wider public benefits, including earthquake monitoring, observation of ocean conditions, and the study of marine ecosystems.

6.3 It also presents national security risks. If accessed by an adversary, sensing data could potentially compromise UK defence interests. Companies deploying sensing technologies are not, on their own, fully sighted on or incentivised to manage the full range of these risks.

6.4 Existing legislation does not provide a coherent basis for managing the risks. Relevant powers under the Marine and Coastal Access Act 2009, the Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021) and the Investigatory Powers Act 2016 are each limited in scope, and none provides a reliable basis on which to ensure this technology is deployed, used or maintained to appropriate and proportionate security standards.

6.5 **For these reasons, the government considers that new primary legislation is required to establish a proportionate security framework for the deployment and operation of subsea fibre-optic sensing technologies.**

Objectives

6.6 We consider the main objectives for new primary legislation should be to:

- i) **Identify and mitigate national security risks** arising from the deployment of sensing technologies before they materialise.
- ii) **Protect sensing data** from hostile access or exploitation.
- iii) **Realise the national security benefits** of sensing technologies through cooperation and data sharing between industry and government.
- iv) **Support the safe and proper use of sensing technologies** rather than discouraging it.

Consultation questions

Q46. Do you agree that new primary legislation is required to establish a proportionate security framework for the deployment and operation of subsea sensing technologies? Please explain your answer.

Q47. Do you agree with the proposed objectives for the regulation of sensing technologies? Please explain your answer.

Overview of proposals

6.7 The government proposes creating a new statutory framework to manage **national security risks associated with the deployment and operation of subsea fibre-optic sensing technologies**. The legislation would be designed to support responsible deployment and use of the technologies.

6.8 This chapter sets out our proposals for the new framework under the following headings:

- i) **Scope**
- ii) **Regulatory regime**
- iii) **Territorial extent**
- iv) **Monitoring and enforcement.**

Scope

Entities in scope

6.9 The government proposes that **responsibility for complying with new legal obligations relating to deployment and use of sensing technologies should rest with the entity that controls the fibre on which the sensing technology is deployed ('the responsible entity')**. That entity is best placed to decide whether and how the technology is deployed, and to meet any legal duties relating to its deployment and use.

6.10 Where sensing technology is deployed, or sensing data⁶ is collected, processed or stored, on the responsible entity's behalf by a third-party supplier or co-owner, the responsible entity would remain responsible for compliance, including through its contractual arrangements.

⁶ Data collected by the sensing technology through its use.

Infrastructure and technologies in scope

6.11 The government proposes that the framework should apply to sensing technologies deployed on optical fibres in subsea cables to detect, measure or analyse activity in the surrounding marine environment. This includes deployments of sensing technologies on fibre integrated into subsea data and energy conveyance systems, as defined in Chapter 2.

6.12 These sensing technologies would include, but not be limited to:

- Distributed Acoustic Sensing (DAS) – uses optical fibre to detect vibrations and acoustic signals along the cable.
- Distributed Temperature Sensing (DTS) – measures temperature variations along the cable.
- Optical Interferometry – detects changes in light phase to infer movement, strain or other environmental conditions.
- State of Polarisation (SoP) sensing – analyses changes in the polarisation state of light travelling through the fibre to detect external influences.⁷

6.13 The framework would not extend to standalone seabed-deployed sensors, buoys or similar equipment that is not integrated into subsea cables. It would also not extend to internal sensing technologies used only to monitor the condition or performance of the infrastructure itself.

6.14 The government proposes a delegated power to set out and amend in secondary legislation a list of the specific technologies in scope. This list would be non-exhaustive and informed by structured engagement with industry across the telecommunications and energy sectors. It would include the technologies described above, together with sensors integrated into cable repeaters or other in-line equipment, and the definition in legislation would be drafted in sufficiently generic terms to accommodate future technologies such as quantum sensing.

Consultation questions

Q48. Do you agree that responsibility should rest with the entity that controls the fibre on which the sensing technology is deployed? Please explain your answer.

Q49. Do you agree with the proposed scope? Are there infrastructure types or technologies not listed that should be included? Please explain your answer.

Q50. Do you agree with the proposal for the government to have a delegated power to set out and amend in secondary legislation a list of the specific technologies in scope? Please explain your answer.

Q51. Please let us know of any further views you have on the proposed scope of the statutory framework.

⁷ These reflect the principal sensing technologies identified by the International Cable Protection Committee (ICPC) – <https://www.iscpc.org/publications/icpc-viewpoints/as-fibreoptic-sensing-in-submarine-cables-develops-rapidly-governments-should-exercise-restraint-in-regulating>.

Regulatory regime

6.15 The government proposes a two-part regulatory regime for subsea sensing technologies. The first part is a screening regime, through which the government would have advance sight of deployments and be able to act to address any specific national security risks a particular deployment presents. The second is a set of baseline security requirements applying to every deployment, ensuring consistent security and resilience standards are applied to the use of the technology and the data it generates.

Screening regime

6.16 Under the screening regime, the responsible entity would be required to notify the government in advance of any sensing technology deployment. Notification would ensure that the government has sight of all deployments and can assess whether those deployments pose national security risks. The notification would include information on:

- **Who** owns and operates the subsea infrastructure upon which the sensing technology is to be deployed, and, if different, who supplies and operates the sensing technology, including details of any third parties with access to the data it collects;
- **What** type of sensing technology is to be deployed, its capabilities and intended use, the data format (raw or processed), sample rate, spatial resolution, frequency range and data retention plans; and
- **Where** the technology is to be deployed, including the location of any interrogator units⁸.

6.17 Responsible entities would not need to wait for the government to finish its review before proceeding with a deployment, aside from in the exceptional circumstances where the government issues an interim order (see below). This is intended to give the government the visibility it needs without unnecessarily creating commercial delays.

6.18 To ensure the requirement is proportionate, different notification timeframes would apply depending on the type of deployment:

Type of deployment	Proposed notification approach
Permanent deployment on existing infrastructure	Notification no less than six months before intended deployment.
New subsea cable or pipeline with integrated sensing technology deployment	Notification during the planning stage, combined with the process for obtaining a licence from the relevant marine licensing authority (telecoms) or approval through the Nationally Significant Infrastructure Projects process (energy), typically at least 12 months before installation begins.
Existing deployments (pre-legislation)	Notification as soon as possible and no later than within 90 days of the relevant provisions entering into law.
Removal, significant modification or upgrade, or change of supplier	Six months' notice.

6.19 Sensing technology may need to be deployed at short notice — for example, to locate a cable fault. To ensure such deployments are not delayed significantly, a provisional notice could be submitted in advance, confirming that sensing may at some future point be deployed

⁸ The device connected to an optical fibre, typically at a cable landing station, which sends light pulses through the fibre and analyses the returning signals to detect and measure activity in the surrounding environment.

on a particular cable, and including all the relevant information. The government would carry out its assessment on receipt of that notice, so that only a short activation notice is required if and when deployment goes ahead. The government proposes an activation period of no fewer than 72 hours for such cases.

Government review process

6.20 The government would review each notification it receives to assess whether the deployment poses any specific national security risks that cannot be adequately managed through the baseline requirements (see below). This review would primarily have regard to:

- the identity of the owner, operator or supplier and any links to any hostile actor;
- the technical capabilities of the sensing deployment; and
- the location of the deployment.

6.21 Most deployments will not present a national security risk and would be reviewed swiftly. **To minimise uncertainty, the government proposes a maximum review period of six months for permanent deployments on existing infrastructure. For new cables where integrated sensing capability is planned from the outset – for instance sensing technology integrated into the repeaters – the government proposes aligning its assessment with the existing marine licensing or Nationally Significant Infrastructure Project processes, so that the review forms part of the overall regulatory assessment and does not add delay.**

6.22 As part of its review, the government proposes that it should have new powers to enable it to obtain further information from the responsible entity to inform its decision-making where necessary, including powers to:

- require additional information from the responsible entity;
- conduct inspections on premises where the sensing technology is to be deployed; and
- in exceptional cases, issue an interim order prohibiting deployment until the review concludes, where there is an imminent threat to national security.

Consultation questions

Q52. Do you agree with the information that responsible entities would be required to provide in a sensing technology deployment notification? Please explain your answer.

Q53. Do you agree with the proposed notification timeframes for different categories of sensing technology deployment? Please explain your answer.

Q54. Do you agree with the proposed provisional notice model for urgent deployments? Please explain your answer.

Q55. Do you agree that the government should have powers to require additional information, undertake inspections and issue interim orders where necessary? Please explain your answer.

Q56. Do you agree with the proposed review criteria? Is anything missing? Please explain your answer.

Intervention powers

6.23 Where a review identifies a significant risk to national security associated with a deployment, the government would have the power to impose bespoke conditions on that deployment through an intervention power. Any conditions would have to be necessary to mitigate the risk identified and proportionate to it. Conditions might, for example, relate to how the technology is configured or the procedures to be followed in operating it.

6.24 In rare cases, where the government determines that there are no conditions under an intervention power that can adequately mitigate the national security risk, the government proposes that the power could be used to prohibit a deployment entirely, provided it is necessary and proportionate to do so in the interests of national security.

6.25 New conditions could be issued by the government, or existing conditions could be varied or reissued, where there is a material change to a deployment, and/or new national security risks emerge in relation to an existing deployment — for example, where there is a change of supplier that presents a national security risk, where the technology is significantly upgraded, or where new risks emerge. This ensures the framework can respond to changes over the life of a deployment rather than only at the point of notification.

Consultation questions

Q57. Do you agree that the government should have the power to issue conditions, and if necessary, prohibit a deployment entirely? Please explain your answer.

Q58. Do you agree with the proposed approach to varying or reissuing conditions where there is a material change to a deployment or new national security risks emerge in relation to an existing deployment? Please explain your answer.

Baseline security requirements

6.26 Irrespective of any bespoke conditions imposed following the review process, responsible entities would be required to comply with a set of baseline security requirements. These measures would help ensure security risks are managed appropriately and proportionately. They would cover both the protection of the technology and its data, and the provision of that data to the government when it considers it necessary and proportionate to do so.

Security and resilience duties

6.27 The government proposes placing, in primary legislation, overarching security and resilience duties on responsible entities. These duties would require them to:

- identify the risks of security compromise affecting the sensing technology and any data it generates;
- take appropriate and proportionate measures to reduce those risks;
- prepare for security compromises, including through incident management arrangements;
- respond to security compromises when they occur, including by containing, mitigating and remediating their effects; and
- comply with government requests for data generated by the sensing technology.

6.28 These duties would apply however the technology is deployed and wherever the data is held, including where sensing data is processed or stored in the cloud.

Powers to make regulations and issue codes of practice

6.29 The government proposes a power to make regulations in secondary legislation setting out specific measures required to meet these duties, and that it should be able to issue codes of practice providing technical guidance on how to comply with the duties. These would be developed in consultation with industry and could be updated as the technology and the threat picture evolve. Examples of the types of measures that might be included in regulations and/or a code of practice include:

Cyber security of sensing technology

- implementation of appropriate network security controls, including firewalls, intrusion detection and intrusion prevention measures;
- timely identification, remediation and patching of vulnerabilities affecting sensing technology and associated infrastructure;
- continuous monitoring, logging and incident response arrangements to detect, investigate and respond to cyber security incidents.

Physical security of sensing technology

- forced entry resistant external doors and windows, and CCTV, lighting and electronic access-control systems with alarms covering all external elevations and entry points;
- housing of sensing equipment within a dedicated, locked internal cage, modular unit or secure room separated from the wider facility, tested or certified to an appropriate recognised standard.

Data security

- encryption of sensing data both at rest and in transit;
- segregation of sensing data processing and storage systems from corporate IT and other operational systems;
- controls on the locations, including cloud and other hosted environments, in which sensing data may be stored or from which it may be accessed.

Data sharing with government

- establishment and maintenance of mechanisms for sharing sensing data with the government in the form and at the frequency requested.

Personnel and supply chain security

- access to sensing technology and data restricted to vetted and authorised personnel;
- maintenance of a record of all personnel with access, to be shared with the government on request;
- regular review of access permissions and prompt removal where no longer required.

Incident reporting

- prompt notification to the government, and in any event within a specified period, of any security incident affecting sensing technology or data, or any unauthorised access to, tampering with, or compromise of it.

Consultation questions

Q59. Do you agree with the proposed approach of setting baseline security requirements on responsible entities deploying sensing technologies? Please explain your answer.

Q60. Do you agree that responsible entities should be required to provide sensing data to government when requested in the interests of national security? Please explain your answer.

Q61. Do you agree that detailed security requirements should be set out through regulations in secondary legislation rather than in primary legislation? Please explain your answer.

Q62. Do you agree that government should be able to issue codes of practice providing technical guidance on compliance with the statutory duties and regulatory requirements? Please explain your answer.

Q63. Do you agree that the illustrative examples of baseline requirements are appropriate and proportionate? Please explain your answer.

Q64. Are there any additional security requirements that should be included, or any proposed requirements that you consider unnecessary or disproportionate?

Territorial extent

6.30 The government proposes that the framework should apply to sensing technologies deployed on optical fibres in subsea cables that connect directly to the UK, where that sensing technology is capable of detecting activity within the UK's territorial sea, exclusive economic zone (EEZ) or continental shelf. Accordingly, a deployment that is not capable of detecting activity within UK waters would fall outside the scope of the framework. For example, sensing technology deployed at the non-UK end of a cable or in the high seas would not be in scope if it cannot detect activity within the UK's territorial sea, EEZ or continental shelf.

6.31 This approach recognises that a sensing deployment cannot sensibly be divided by reference to maritime boundaries. The interrogation equipment may be located at a landing station in the UK, while sensors may be integrated into repeaters beyond the territorial sea, and the data generated may be processed or stored elsewhere. Defining the scope of the framework by reference to a deployment's ability to detect activity within UK waters therefore provides a clearer and more effective basis for regulation than relying on the location of individual components. Any obligations applying to such deployments would be exercised consistently with international law.

6.32 The government also proposes that the framework captures deployments on optical fibres in subsea cables that pass through UK waters but do not directly connect to the UK mainland, where those deployments are capable of detecting activity within the UK's territorial sea, EEZ or continental shelf. Such deployments are equally capable of revealing UK military patterns of activity in or around UK waters and may therefore present similar national security risks to deployments on cables that directly connect to the UK. The government considers that this provides a sufficient connection to the United Kingdom to justify their inclusion within the framework. As above, any obligations applying to such deployments would be exercised consistently with international law.

Consultation questions

Q65. Do you agree with the proposed territorial extent of the framework? Please explain your answer.

Q66. Do you agree that the framework should apply to sensing technology deployments on subsea cables that pass through UK waters but do not directly connect to the UK, where they are capable of detecting activity within the UK's territorial sea or EEZ? Please explain your answer.

Q67. Please let us know of any further views you have on the proposed territorial extent of the sensing framework, including on practicality of implementation.

Monitoring and enforcement

6.33 The framework would create enforceable obligations under both the screening regime and the baseline security requirements, with enforcement and penalty provisions applying to both.

6.34 Under the screening regime, enforceable obligations would include:

- the requirement to notify the government of a sensing deployment within the applicable timeline, including through provisional and activation notices;
- the requirement not to proceed with a deployment in breach of an interim order; and
- compliance with any bespoke condition imposed, or prohibition made, following the government's review of a notification.

6.35 Under the baseline security requirements, enforceable obligations would include the overarching security duties and any specific requirements set out in regulations.

6.36 In addition, the government proposes that it should be an enforceable contravention to provide false or misleading information in a notification or in response to an information notice, or to obstruct a lawful inspection.

6.37 For breaches of either the screening regime or the baseline requirements, the government proposes a civil enforcement model. The enforcement authority would monitor and assess compliance, require action to be taken where obligations are not being met, and impose financial penalties. Financial penalties would include a specified percentage of relevant annual turnover, together with daily penalties for continuing contraventions. The government would also be able to seek enforcement through civil proceedings, including injunctions, where necessary to protect national security.

6.38 The government considers there may also be a case to include criminal penalties for the most serious breaches — for example, deliberate non-compliance that endangers national security.

6.39 The government is considering precisely how compliance with the screening regime and the baseline security requirements should be monitored and enforced. While bespoke conditions would be imposed on a case-by-case basis and baseline requirements would apply more broadly across those deploying sensing technology, the government considers it important that appropriate arrangements are in place to assess compliance and respond where obligations are not being met. The government will confirm the approach when it publishes its response to this consultation.

Consultation questions

Q68. Do you agree with the proposed enforceable obligations? Please explain your answer.

Q69. Is the proposed approach to penalties appropriate and proportionate? Please explain your answer.

Q70. Is there a case for criminal penalties for the most serious breaches? Please explain your answer.

Q71. Please let us know of any further views you have on the proposed enforceable obligations, penalties and enforcement arrangements.

Annex A: How to respond and next steps

The government welcomes views from anyone with an interest in the proposals within this White Paper, including individuals, industry, academia, and civil society organisations.

Consultation questions are included throughout the White Paper. The same questions are also listed in full in **Annex B** of the White Paper. Respondents are encouraged to answer any questions relevant to their knowledge and expertise. We encourage respondents to provide not just their opinions, but also supporting facts and reasoning to inform the evidence base for the development of our proposals. We welcome views on specific proposals and broader views on the proposed legislation as a whole.

The consultation will be open for 12 weeks, from Thursday 22 October 2026 to 23:59 on Thursday 14 January 2027.

You can respond online via the following link:

<https://www.smartsurvey.co.uk/t/cuillegislationconsultation/>

When responding, please state whether you are responding as an individual or representing the views of an organisation.

In exceptional circumstances, if you need to submit a hard copy response or require another format (e.g. braille or large font) please contact cui.legislation.consultation@DSIT.gov.uk.

We recognise that proposals set out in this White Paper could potentially impose significant costs on affected businesses. The government is seeking evidence on these potential costs to inform its assessment of the economic impacts of the proposals. **You can provide us with information on the potential costs of the proposals to you, or your organisation, by completing an online cost impact survey via the following link:**

https://www.smartsurvey.co.uk/t/subsea_cable_legislation_review_cost_impact_survey/

Following the closure of the consultation, the government will carefully consider all responses received to inform further development of the legislation proposals. We will also continue to engage with a range of stakeholders – including regulators, industry stakeholders and international partners – to refine the proposals.

We will publish the government's response to this consultation on the GOV.UK website, summarising the responses received and setting out the action we will take, or have taken, in respect of them in developing our final proposals for legislation. Following the publication of the government's response, we plan to bring forward legislation when parliamentary time allows.

Annex B: Consultation Questions

This annex lists all consultation questions in the order in which they appear in the White Paper. Guidance on how to respond to the consultation is provided in **Annex A** of the White Paper.

Chapter 2: Key Terms

No.	Question
1	Do you agree with the proposed terms and definitions in this chapter? Please explain your answer.

Chapter 3: Criminal penalties regime

No.	Question
Objectives	
2	Do you agree that new primary legislation is required to modernise and strengthen UK legislation to protect CUI and deter harmful conduct effectively? Please explain your answer.
3	Do you agree with the proposed objectives for the criminal penalties regime? Please explain your answer.
New offences	
4	Do you agree with the proposed approach to the offence framework? Please explain your answer.
5	Please let us know of any further views you have on the proposed offences.
Penalties and liability	
6	Do you agree with the proposed approach to penalties and liability? Please explain your answer, including any views on proportionality and deterrence.
7	Please let us know of any further views you have on the proposed penalties.
Territorial extent	
8	Do you agree with the proposed territorial extent? Please explain your answer.
Enforcement	
9	Do you agree with the proposed approach to enforcement? Please explain your answer.

No.	Question
10	Do you think any changes to existing enforcement powers are required to give practical effect to the proposed offences? Please explain your answer.
11	Please let us know of any further views you have on enforcement.

Chapter 4: Security and resilience duties

No.	Question
Objectives	
12	Do you agree that new duties in primary legislation on providers of subsea data conveyance systems and services are required to establish clear and consistent security and resilience standards? Please explain your answer.
13	Do you agree with the proposed objectives for the security and resilience duties? Please explain your answer.
Duties on providers	
14	Do you agree with the proposal to introduce the following security and resilience duties: • duty to take appropriate and proportionate measures to manage the risk of security compromise; • duty to take measures in response to security compromises; • duty to notify government and the appropriate regulator of any security compromise; • duty to inform others of significant risk of security compromise? Please explain your answer.
15	What are your views on whether a registration requirement should be introduced for the providers of subsea data conveyance systems or services?
16	Please let us know of any further views you have on the proposed duties, including if you think anything is missing.
Secondary legislation and codes of practice	
17	Do you agree that detailed security and resilience requirements should be set out in regulations within secondary legislation? Please explain your answer.
18	Do you agree that government should be able to issue codes of practice providing guidance on how providers can comply with their duties and regulatory requirements? Please explain your answer.
19	Please let us know of any further views you have on the proposed use of secondary legislation and codes of practice.
Entities, systems and services in scope	
20	Do you agree with the proposed approach to the providers in scope of the security and resilience duties? Please explain your answer.
21	Do you agree with the proposed approach to the systems and services in scope of the security and resilience duties? Please explain your answer.
22	Do you agree with the proposed approach for avoiding dual regulation? Please explain your answer.
23	Please let us know of any further views you have on the scope of the duties.

No.	Question
Territorial extent	
24	Do you agree that the duties should apply within the UK's territorial sea? Please explain your answer.
25	Please let us know of any further views you have on the proposed territorial extent of the security and resilience duties.
Monitoring and enforcement	
26	Do you agree with the proposed monitoring and enforcement powers? Please explain your answer.
27	Are there any additional monitoring or enforcement powers that should be available to the regulator? Please explain your answer.
28	Please let us know of any further views you have on the proposed monitoring and enforcement proposals.

Chapter 5: National security direction power

No.	Question
Objectives	
29	Do you agree that new primary legislation is required to enable the government to compel action in specific circumstances in the interests of national security? Please explain your answer.
30	Do you agree with the proposed objectives of the national security direction power? Please explain your answer.
Entities in scope	
31	Do you agree with the proposed entities in scope? Are there other entities that should be within scope? Please explain your answer.
32	Please let us know of any further views you have on the entities in scope of the power.
Direction power	
33	Do you agree with the proposed threshold for exercising the direction power, namely that the Secretary of State must be satisfied that a compromise of, or threat to, a subsea data conveyance system or service gives rise to a risk to national security? Please explain your answer.
34	Do you agree with the types of requirements a direction could impose that we have proposed? Please explain your answer.
35	Do you agree with the proposed safeguards on the exercise of the direction power? Are any additional safeguards needed? Please explain your answer.
36	Do you agree with the proposal that compliance with a direction should generally take precedence over other requirements in legislation, provided such compliance is compatible with the government's international law obligations? Please explain your answer.
37	Do you agree with the proposed standing power for the Secretary of State to require information from entities in scope to help the government maintain an accurate understanding of the sector? Please explain your answer.
38	Please let us know of any further views you have on the direction power itself.
Territorial extent	
39	Do you agree with the proposed territorial extent of the power, including that a direction may have effect beyond the UK's territorial sea? Please explain your answer.

No.	Question
40	Do you agree with the proposal that a direction may have effect along the full extent of the system or service, including beyond the UK's territorial sea, where the national security risk or impact arises in relation to the UK? Please explain your answer.
41	Do you have views on how use of the power should be coordinated with other states that share subsea systems connecting to the UK? Please explain your answer.
42	Please let us know of any further views you have on the proposed territorial extent of the power.
Monitoring and enforcement	
43	Do you agree with the proposed approach to monitoring and enforcement? Please explain your answer.
44	Do you think the proposed financial penalties are appropriate and proportionate? Please explain your answer.
45	Please let us know of any further views you have on monitoring and enforcement of compliance with the directions that would be issued under the proposed power.

Chapter 6: Regulation of sensing technologies

No.	Question
Objectives	
46	Do you agree that new primary legislation is required to establish a proportionate security framework for the deployment and operation of subsea sensing technologies? Please explain your answer.
47	Do you agree with the proposed objectives for the regulation of sensing technologies? Please explain your answer.
Scope	
48	Do you agree that responsibility should rest with the entity that controls the fibre on which the sensing technology is deployed? Please explain your answer.
49	Do you agree with the proposed scope? Are there infrastructure types or technologies not listed that should be included? Please explain your answer.
50	Do you agree with the proposal for the government to have a delegated power to set out and amend in secondary legislation a list of the specific technologies in scope? Please explain your answer.
51	Please let us know of any further views you have on the proposed scope of the statutory framework.
Screening regime	
52	Do you agree with the information that responsible entities would be required to provide in a sensing technology deployment notification? Please explain your answer.
53	Do you agree with the proposed notification timeframes for different categories of sensing technology deployment? Please explain your answer.
54	Do you agree with the proposed provisional notice model for urgent deployments? Please explain your answer.
55	Do you agree that the government should have powers to require additional information, undertake inspections and issue interim orders where necessary? Please explain your answer.

No.	Question
56	Do you agree with the proposed review criteria? Is anything missing? Please explain your answer.
57	Do you agree that the government should have the power to issue conditions, and if necessary, prohibit a deployment entirely? Please explain your answer.
58	Do you agree with the proposed approach to varying or reissuing conditions where there is a material change to a deployment or new national security risks emerge in relation to an existing deployment? Please explain your answer.
Baseline security requirements	
59	Do you agree with the proposed approach of setting baseline security requirements on responsible entities deploying sensing technologies? Please explain your answer.
60	Do you agree that responsible entities should be required to provide sensing data to government when requested in the interests of national security? Please explain your answer.
61	Do you agree that detailed security requirements should be set out through regulations in secondary legislation rather than in primary legislation? Please explain your answer.
62	Do you agree that government should be able to issue codes of practice providing technical guidance on compliance with the statutory duties and regulatory requirements? Please explain your answer.
63	Do you agree that the illustrative examples of baseline requirements are appropriate and proportionate? Please explain your answer.
64	Are there any additional security requirements that should be included, or any proposed requirements that you consider unnecessary or disproportionate?
Territorial extent	
65	Do you agree with the proposed territorial extent of the framework? Please explain your answer.
66	Do you agree that the framework should apply to sensing technology deployments on subsea cables that pass through UK waters but do not directly connect to the UK, where they are capable of detecting activity within the UK's territorial sea or EEZ? Please explain your answer.
67	Please let us know of any further views you have on the proposed territorial extent of the sensing framework, including on practicality of implementation.
Monitoring and enforcement	
68	Do you agree with the proposed enforceable obligations? Please explain your answer.
69	Is the proposed approach to penalties appropriate and proportionate? Please explain your answer.
70	Is there a case for criminal penalties for the most serious breaches? Please explain your answer.
71	Please let us know of any further views you have on the proposed enforceable obligations, penalties and enforcement arrangements.
Further views on the proposals	
72	Should you have any further views on the proposals set out in this White Paper please let us know.

