



CabinetOffice

Strategic Framework and Policy Statement

on Improving the Resilience of Critical Infrastructure
to Disruption from Natural Hazards

March 2010

Produced by:

Cabinet Office
22 Whitehall
London
SW1A 2WH

Web address: www.cabinetoffice.gov.uk

Contact:

Natural Hazards Team
Civil Contingencies Secretariat
naturalhazards@cabinet-office.x.gsi.gov.uk

Publication date: March 2010

© Crown copyright 2010

The text in this document may be reproduced free of charge in any format or media without requiring specific permission. This is subject to it not being used in a derogatory manner or in a misleading context. The source of the material must be acknowledged as Crown copyright and the title of the document must be included when reproduced as part of another publication or service.

CONTENTS

1. INTRODUCTION

Purpose

Background

2. THE CRITICAL INFRASTRUCTURE RESILIENCE PROGRAMME

Definitions

Aims

Principles

Scope

Work Streams

Timetable

3. POLICY AND STANDARDS

The Impact of Natural Hazards

Flood Resilience Standards

4. ROLES AND RESPONSIBILITIES

Cabinet Office

Government Departments

Devolved Administrations

Regulators

Infrastructure owners and operators

Centre for the Protection of National Infrastructure

Environment Agency

Annex A: Categorising infrastructure and the criticality scale

FOREWORD

Sir Michael Pitt identified during the review of the summer 2007 floods, a gap in the Government's policy-making and delivery towards the protection of critical infrastructure from severe disruption caused by natural hazards.

In his Interim Report, Sir Michael concluded "that the Government should establish a systematic, coordinated, cross-sector campaign to reduce the disruption caused by natural events to critical infrastructure and essential services."

This Strategic Framework and Policy Statement (the Framework) sets out proposals for a cross-sector systematic programme to improve the resilience of critical infrastructure and essential services to severe disruption by natural hazards (the Programme). It covers the proposed policy intent, scope, aims, timescales and work streams.

The Framework establishes an interim standard for resilience for critical infrastructure in relation to flooding. This will be the basis for developing the evidence base on the practicalities, costs and benefits of setting resilience standards for all natural hazards. The final resilience standards will be set out in a National Resilience Plan for Critical Infrastructure to be published in 2011. This Plan will be supported by an impact assessment.

The Government believes that better knowledge and awareness of the vulnerability of critical infrastructure within Government,

regulators and infrastructure owners will drive a programme to improve resilience to determined standards.

In addition to this Framework, the Cabinet Office has issued separate guidance to economic regulators on how they can support a programme of resilience building.



Christina Scott
Director – Civil Contingencies Secretariat

SECTION 1: INTRODUCTION

Purpose

1.1 This Strategic Framework and Policy Statement establishes a cross-sector programme to improve the resilience of critical infrastructure and essential services to disruption from natural hazards. The purpose is to develop a shared, consistent, proportionate and risk-based approach to delivering reductions in vulnerability over a number of years, as envisaged by Sir Michael Pitt in his reports on the floods of summer 2007.

1.2 As Sir Michael recommended, the Framework is intended to encompass a co-ordinated approach to driving up the resilience of critical infrastructure. The main goal is to identify and assess risks from natural hazards, and thereafter to develop a range of options to avoid, transfer, accept, reduce or share those risks. Options could vary from the provision of physical protection through the relocation of assets, or the provision of alternative supplies, or improved arrangements for emergency response.

1.3 This Framework is primarily directed at central government departments, regulators, relevant public sector bodies and critical infrastructure owners. It describes the policy intent, scope, aims, work streams and timescales of the Critical Infrastructure Resilience Programme. This Framework aims to:

- Embed a co-ordinated and systematic approach to improve resilience of the infrastructure network and systems that

provide essential services to severe disruption from natural hazards (Section 2).

- Establish an interim minimum standard for resilience to flooding (Section 3).
- Clarify the roles and responsibilities of the wide range of public and private sector bodies who will contribute to the delivery of the shared goals of the Programme (Section 4).

Background

1.4 Sir Michael Pitt identified in his report on the summer 2007 floods a gap in the Government's policy-making and delivery towards the protection of critical infrastructure from severe disruption caused by natural hazards. In his Interim Report, Sir Michael concluded: "that the Government should establish a systematic, coordinated, cross-sector campaign to reduce the disruption caused by natural events to critical infrastructure and essential services."

1.5 Sir Michael found that a number of factors appeared to work together to reduce the effectiveness of risk mitigation within critical infrastructure sectors:

- a. The Centre for the Protection of National Infrastructure (CPNI) provides protective security advice aimed at reducing the vulnerability of critical national infrastructure to national security threats but has no such role in relation to natural hazards.
- b. Although information is available on actual risks arising from extreme weather conditions and other related natural hazards, and increasingly on future changes in mean climate parameters, information on future extreme weather events is poorly understood.
- c. There is no systematic shared understanding of the scale of vulnerability in

each sector or of critical infrastructure as a whole to natural hazards.

d. Whilst a number of policies and programmes are in place which will help to drive risk mitigation in a number of infrastructure sectors, the framework is patchy and inconsistent. Much of what is presently being done is the product of ad hoc reactions to specific events or particular administrative processes.

1.6 Sir Michael, in his Final Report, set out five recommendations to guide the cross-sector campaign described above:

- Recommendation 50: The Government should urgently begin its systematic programme to reduce the disruption of essential services resulting from natural hazards by publishing a national framework and policy statement setting out the process, timescales and expectations.
- Recommendation 51: Relevant government departments and the Environment Agency should work with infrastructure operators to identify the vulnerability and risk of assets to flooding and a summary of the analysis should be published in Sector Resilience Plans.
- Recommendation 52: In the short-term, the Government and infrastructure operators should work together to build a level of resilience into critical infrastructure assets that ensures continuity during a worst case flood event.
- Recommendation 53: A specific duty should be placed on economic regulators to build resilience in the critical infrastructure.

- Recommendation 54: The Government should extend the duty to undertake business continuity planning to infrastructure operating Category 2 responders to a standard equivalent to BS 25999, and that accountability is ensured through an annual benchmarking exercise within each sector.

1.7 In its response, the Government supported Recommendations 50, 51, 52 and 54, and the aims of recommendation 53.

SECTION 2:

THE CRITICAL INFRASTRUCTURE RESILIENCE PROGRAMME

Definitions

Resilience

2.1 In his report, Sir Michael Pitt defined resilience as “the ability of a system or organisation to withstand and recover from adversity.” As such, a resilient organisation is one that is still able to achieve its core objectives in the face of adversity through a combination of measures.

2.2 Sir Michael also noted that: “protection may make up an important part of resilience, but it is not the only factor. Resilience is also underpinned by an effective emergency response to help reduce the impacts of failure”.

2.3 In the Government’s view, resilience encompasses activity to prevent, protect and prepare for natural hazards. It is important to get the balance right between investment in critical infrastructure itself and investment in emergency response and recovery capabilities and plans. A programme to improve resilience within the UK’s critical infrastructure will need to encompass prevention, protection, response and recovery. In an increasingly networked society, it will also need to take account of

dependencies and interdependencies within and between sectors.

2.4 Critical infrastructure operators and providers of essential services will need to consider a range of options for ensuring continuity of supply, including:

- Considering the threat from current and future natural hazards in the design of new assets, networks and systems to avoid disruption arising in the first place.
- Increasing the robustness and resilience of existing services or assets by building additional network connections, or by providing backup facilities to ensure continuity of services. Actions may include protection measures such as permanent or temporary flood defences.
- Identifying key components and moving them out of harm’s way. For example, by moving high-criticality assets that are vulnerable to flooding into a lower-risk area. For most infrastructure assets, relocation can only be a longer-term option, meaning that short-term measures may be needed to buy time to plan for the necessary change.
- Improved arrangements for sharing of information on infrastructure network performance and standards.
- Enhancing skills and capabilities to respond to emergencies arising from natural hazards.

Risk

2.5 In this Framework, risk is defined as a product of the likelihood of a disruptive event occurring and the disruptive impact that it would have. Risk assessment is the process to identify the likelihood of hazards occurring and the corresponding impacts.

National Infrastructure and Critical National Infrastructure

2.6 The UK's national infrastructure is defined by the Government as: "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends".

2.7 There are certain "critical" elements of national infrastructure that if lost would lead to severe economic or social consequences or to loss of life in the UK. These critical elements make up the critical national infrastructure (CNI).

Critical National Infrastructure

The Government defines CNI as: "Those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life"

2.8 The National Infrastructure is categorised into nine sectors: energy, food, water, transportation, communications, emergency services, health care, financial services and government. There are some cross-sector themes such as technology wherein there may be infrastructure which supports the delivery of essential services across a number of sectors. Annex A provides further information on the UK's national infrastructure sectors, sub-sectors and the system for categorising infrastructure.

2.9 The European Union defines critical infrastructure in a broadly similar way: "Critical infrastructure (CI) consists of those physical and information technology facilities, networks, services and assets which, if

disrupted or destroyed, have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments".

2.10 These definitions are important to ensure clarity and consistency when considering whether infrastructure is critical. From the perspective of the consumer, what matters is the loss of an essential service, irrespective of whether it arises from the loss of either national or local infrastructure assets. For the purposes of the Programme there are:

- (a) critical national infrastructure (that is, infrastructure which is deemed critical on a national scale); and
- (b) other critical infrastructure which may be critical within a local area.

This will enable assets, systems or networks not otherwise deemed as critical national infrastructure to be evaluated and included within the Programme if doing so would be appropriate and proportionate. However, the risk-based approach that underpins the Programme means that initial vulnerability analysis will focus on the Critical National Infrastructure.

Aims

2.11 The aims of the Critical Infrastructure Resilience Programme are to:

- Reduce the most substantial risks to the continuity of critical infrastructure and essential services resulting from severe disruption caused by natural hazards, through the careful assessment of vulnerability and prudent and proportionate risk mitigation activity based on new, centrally-defined standards.
- Provide a shared framework to support cross-sector activity to assess, enhance and sustain the resilience of critical infrastructure and essential services to disruption from natural hazards.
- Enhance the collective capacity of critical infrastructure to absorb shock and act quickly when faced with unexpected events.
- Ensure an effective emergency response at the local level through improved information sharing and engagement before, during and after emergencies.

2.12 The Programme will ensure that the Government, regulators, public sector bodies and owners of critical infrastructure are aware of the risks arising from natural hazards and take appropriate action. This includes understanding the potential impact on society, the economy and the environment. This information, alongside defined standards for resilience, will enable plans to be developed to manage the risks and improve the resilience of critical infrastructure and essential services.

Principles

2.13 The Programme will be based on the following principles:

- **Risk-based approach.** The standards adopted and measures proposed to enhance resilience will be proportionate to the risks posed by natural hazards. Assessments of the likelihood and the consequences of critical infrastructure and essential services being severely disrupted by natural hazards will be used to define standards and set priorities.
- **Proportionality.** The scale and cost of proposed programmes of measures to enhance resilience within each sector should be proportionate to the risks they face. This means taking into account the likelihood of their being affected by a natural hazard, the “criticality” of the infrastructure in question and its vulnerabilities, and the different options available to improve resilience.
- **Co-operation and co-ordination.** The Programme will encourage and facilitate co-ordination and integration within and between sectors and essential services to deliver the aims set out above. It will also be based on collaboration with similar programmes within the Devolved Administrations on matters that are devolved, and respect the roles of each Administration. Arrangements will be established with the Devolved Administrations to harmonise work programmes where possible to ensure appropriate standards for resilience are progressed across the UK.
- **Sector differences.** Sector Resilience Plans will clarify the differences between sectors that arise from their different needs, circumstances and regulations,

which will be taken into account in the National Resilience Plan for Infrastructure.

- **Sector sponsor department responsibility.** Lead Government Departments will continue to sponsor and take the lead for their sectors, although the responsibility for the resilience of essential services remains with the owners of critical infrastructure. Where a sector is devolved the devolved administration in question has the functions of a lead government department.
- **Coherence.** Proposed Sector Resilience Plans should be “joined-up” as far as possible with other relevant Government programmes, especially the programme to reduce the vulnerability of critical national infrastructure to terrorist attacks and reporting on adaptation to climate change under the Climate Change Act 2008.
- **Voluntary co-operation.** This will be the preferred means of achieving shared aims, although the use of guidance, regulatory or other legislative powers may be appropriate or necessary.
- **Tripartite relationship.** The Programme will seek to establish a tripartite relationship between the sector sponsoring department, the relevant regulator and infrastructure owners in taking activity forward, where relevant.
- **Information sharing.** The Programme will promote appropriate information sharing to support resilience-building, especially on dependencies, interdependencies and arrangements for business continuity management across sectors.
- **Precautionary.** A precautionary approach will be taken to encompass inherent uncertainties in the estimation of the risks posed by natural hazards across the medium-term.

- **Sustainability.** Programmes of resilience-building will be scrutinised for their contribution towards the Government’s aims for sustainable development, especially the creation of safe and sustainable communities. Individual resilience-building measures will need to support National Planning Statements, be consistent with spatial plans and comply with planning policies (e.g. Planning Policy Statement 25 on Development and Flood Risk).

Scope

2.14 The Programme will cover all nine sectors of national infrastructure. It will reflect the position that each sector is at a different starting point. As a result, expectations for each sector will be different in the early stages of the Programme. Some sectors are devolved to Scotland, Wales and Northern Ireland. In these cases the devolved administration in question is responsible for ensuring resilience. The programme will work in partnership with the devolved administrations to adopt where appropriate a common approach.

2.15 Many critical infrastructure owners already have in place arrangements for improving and sustaining the resilience of their assets, networks and systems, and for risk assessment and business continuity management. The Programme will work in partnership with those owners, lead government departments and regulators to understand activity already under way, to assess the residual vulnerability of infrastructure assets to severe disruption caused by natural hazards and to determine if further measures are necessary to improve resilience.

2.16 The Government already has in place a comprehensive programme to protect the critical national infrastructure from terrorism as part of the UK's counter-terrorism strategy (CONTEST). Sector sponsor departments are responsible for deciding upon the appropriate security approach to be taken for their sector. The Centre for the Protection of National Infrastructure (CPNI) supports this programme of work. A strategic framework is in place (CNI Protection in the UK: Framework and Guidance) which provides a common foundation for activity by all those involved in national infrastructure protection from counter-terrorism and other national security threats.

2.17 The prepare work under CONTEST is being taken forward by the Cabinet Office to build capabilities within the resilience community to respond to threats and hazards identified in the National Risk Register (NRR). The Critical Infrastructure Resilience Programme will seek to align with the CONTEST strategy. Existing processes and procedures will be adopted where possible to provide a coherent and consistent approach to building resilience across sectors to all risks and threats, including natural hazards.

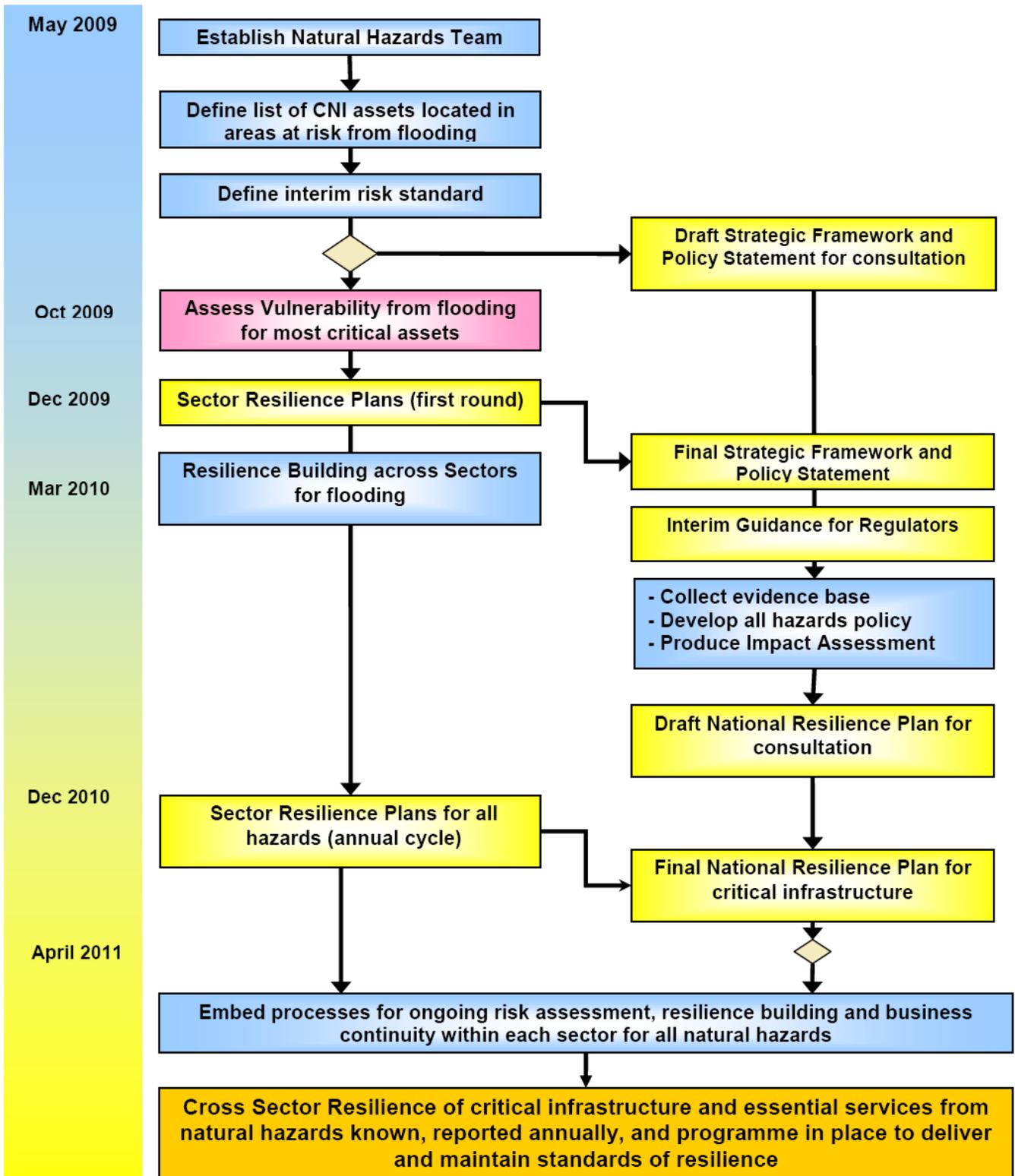
2.18 The Programme will work closely with the Adapting to Climate Change Programme. This is to ensure consistency and pursue how best to align with the reporting obligations under the Climate Change Act, and the reporting requirements under the Flood Risk Regulations 2009.

2.19 The Programme will work closely with Infrastructure UK to ensure that findings feed into the long-term planning and prioritisation of UK infrastructure and work to enable investment in infrastructure and improve delivery.

2.20 The Programme will assess and identify the activity and investment needed to improve resilience to defined standards and set this out in a formal impact assessment. This analysis will be developed, and the supporting evidence gathered, during the consultation on this document and through the development of Sector Resilience Plans. Ministers will make the final decision on resilience standards and delivery mechanisms for resilience programmes in each sector.

2.21 The Programme will be developed to consider all natural hazards. The initial focus will be on flooding from rivers and the sea – see the outline plan in figure 1. Other forms of flooding (including surface water, reservoirs, canals and groundwater) and natural hazards will be incorporated into the sector resilience plans during 2010 and beyond. The process for extending the plans beyond flooding will be a priority for policy development within the Programme.

Figure 1: Outline Programme Plan



Work Streams

2.22 The Programme will be developed in eight work streams:

- Sector Resilience Plans
- Natural Hazards
- Regulation
- Resilience Standards
- Social Requirements for Resilience
- Dependencies and Information Sharing
- Business Continuity
- Impact Assessment

Sector Resilience Plans

2.23 The Pitt Review recommended the development of Sector Resilience Plans as a key element of the programme of “Government and industry working together to foster a collective responsibility for enhancing resilience.” The Report proposed that these plans are “developed jointly through a tripartite relationship between the relevant government department, economic regulator and industry sector, should be public documents with controlled sections where necessary for sensitive information.”

2.24 Sector Resilience Plans are expected in the longer term to set out:

- an understanding of vulnerability and overall risk within the sector, developed by the bottom-up risk assessment and analysis on a periodic basis;
- the levels of ambition for resilience across the sector within a defined timeframe, based on existing standards of protection, economic factors and business continuity planning for all risks;

- a programme of measures for achieving the defined level of ambition, along with timescales for delivery;
- a mechanism for reporting progress on the implementation of the programme of measures, and for updating the plan on an annual basis to incorporate changes in the understanding of risks and actions taken; and
- a process for the benchmarking of business continuity plans.

2.25 Flooding is the first hazard to be considered by these Plans as it is the highest climatic risk in the Government’s National Risk Register. Information is already available on flood risk across the UK that can be used to assess the vulnerability of individual infrastructure assets to severe disruption from flooding and hence the need for activity and investment to reduce those vulnerabilities. Risks posed by other natural hazards are not currently as precisely defined. Where they are, however, they will be taken into account in the vulnerability analysis.

2.26 The Cabinet Office has mapped the critical national infrastructure to determine sites that are located in areas at risk from flooding from rivers or the sea using data from the Environment Agency and CPNI. The lead government departments then developed the first round of the Sector Resilience Plans for these sites. The first versions of the Sector Resilience Plans were delivered in England at the end of December 2009.

2.27 The first version of these plans set out:
(a) the lead government department’s understanding of the risks from river and coastal flooding to critical infrastructure and essential services in their sector;

(b) a clear picture of what is already being done directly and indirectly to address deficiencies in resilience to severe disruption from flooding; and

(c) the further work that will be needed to improve resilience to disruption from flooding to the initial interim standard.

2.28 Future Sector Resilience Plans will be progressively extended to cover all natural hazards and critical infrastructure, and to plan for future climate parameters. Future risks will be drawn from successive versions of the National Risk Register and UK Climate Projections. The Programme will produce guidance to support the progressive development of Sector Resilience Plans.

2.29 Each sector will require an infrastructure-wide iterative process to periodically assess the risk, then plan and deliver actions to improve resilience to achieve and maintain standards expected by communities, regulators (where appropriate) and the Government. Responsibility for producing the Plans will rest with the lead government department for each sector, with information provided by owners of critical infrastructure within the sector. The reporting will be aligned with planning and reporting requirements under the Climate Change Act 2008 and the Flood Risk Regulations 2009 if possible.

2.30 The Pitt Report intended that Sector Resilience Plans are reviewed annually by lead government departments and updated to reflect progress within the sector. The Cabinet Office will establish arrangements for quality assurance of the Plans to ensure that they are fit for purpose, and seek to include monitoring of progress within the existing Capability Programme.

Natural Hazards

2.31 The programme will determine what natural hazards should be included and the approach to be used to effectively expand the programme beyond flooding.

2.32 Initial scoping will focus on those hazards outlined in the National Risk Register: high winds and gales; ice and snow; extremes of hot and cold; and drought.

2.33 Hazards have conventionally been prioritised based on historical evidence, rather than a proactive assessment of actual risk. The programme will look at widening the assessment base for risks, and investigate opportunities to incorporate with the annual review of the National Risk Register.

2.34 During the policy development process, further evidence will be gathered on additional hazards which may need to be taken into account in the National Resilience Plan for Critical Infrastructure.

Regulation

2.35 This Framework provides interim guidance for economic regulators on the Government's expectations for resilience of critical infrastructure from flooding (see section 3). This is in response to recommendation 53 of Sir Michael Pitt's final report.

2.36 The programme will review existing regulation and guidance, identifying best practice and existing gaps in provision. It will also review current affordability appraisal practices in each sector, addressing how any improvements can be funded and whether any legal powers are needed to improve resilience.

2.37 Additional interim guidance providing examples of good practice on resilience and further considerations will be published in

2010. This will enable regulators to consider how they can effectively support a national programme of cross-sector resilience-building from all natural hazards.

Resilience Standards

2.38 An interim minimum standard for flood resilience in critical national infrastructure is set out in section 3 of this Framework. Setting an interim standard at an early stage allows:

- (a) a clear statement of expectation to be made while allowing a period of discussion and evidence-gathering;
- (b) the National Resilience Plan for Critical Infrastructure and Government's policy on resilience to be developed in parallel with the production of Sector Resilience Plans, thus ensuring consistency;
- (c) an assessment of the scale of activity needed to improve the resilience of relevant infrastructure to this standard;
- (d) determination of the costs of setting a particular standard, the investment needed over what timeframe; and hence what will be the impact on owners' (providers') business models and customers' bills.

2.39 The Programme will review existing standards in use across the nine sectors of national infrastructure and evaluate if these can be used to drive resilience, and analyse gaps in provision of appropriate and consistent standards. Opportunities to reduce the regulatory burden on industry will be taken where identified and possible to implement. The review will investigate appropriate and proportionate event and service based standards as well as generic business continuity standards.

2.40 The merits of setting different standards for the most critical assets and within each sector, on economic, social and environmental grounds will be assessed before any recommendations are made.

2.41 The National Resilience Plan for Critical Infrastructure will set out a risk-based approach for resilience-building and set appropriate sector standards, which will be reflected in the regulatory programme.

Social Requirements for Resilience

2.42 The programme will work with the lead government departments and experts to understand the social impact of disruption to essential services from natural hazards. An understanding of public expectations and willingness to pay will be considered in the development of resilience standards and policy.

2.43 The programme will look at recent case studies and the disproportionate impacts on vulnerable groups and work already undertaken by lead government departments in this area.

Dependencies and Information Sharing

2.44 This work stream will consider cross-sector issues arising from the dependency and inter-connectivity of services. It will consider how to identify the potential for, and likelihood of, chains of events that could lead to cascade failures, with a consequent greater impact on communities. Developing a better shared understanding of dependencies across sectors will enable improvement in resilience.

2.45 The focus of work under the Critical Infrastructure Resilience Programme will be

to provide guidance to improve sharing of information between category 1 and category 2 responders under the Civil Contingencies Act 2004. The programme will review current practice on information sharing on critical infrastructure at the national, regional and local level, and how it is being used to plan and improve resilience of infrastructure and essential services.

2.46 The Programme will consider who needs to have a wider understanding of dependencies and interconnectivity of infrastructure and essential services across sectors, what information is needed, and how this knowledge will improve resilience. Guidance for category 1 responders and category 2 responders will be produced, based on current practice and evidence from programme findings, to encourage cooperation and information sharing.

2.47 The Council of Science and Technology Report on “A National Infrastructure for the 21st Century” highlighted that there is a lack of understanding of the vulnerabilities of critical infrastructure, particularly where one sector is dependent on another. Unless addressed, such dependencies can lead to a misplaced level of reliance on other systems that could also have serious consequences. The report recommended more investment by business, the regulators and Government in modelling techniques, to measure, predict and mitigate the functioning and malfunctioning of complex infrastructure systems. The Chief Scientific Adviser to the Department for Business, Innovation (BIS) and Skills and the Department for Transport is taking forward work to develop a national approach to modelling the dependencies of national infrastructure. The Programme will support BIS in this work.

2.48 The Programme will determine the need for infrastructure resilience groups at local

and regional level, and whether a national multi-sector strategic co-ordination and planning group for national infrastructure should be established. Where possible, existing mechanisms, processes and plans will be utilised to facilitate the assessment of vulnerabilities on dependent networks and systems across sectors.

Business continuity

2.49 The Government supports the Pitt Recommendation 54 to extend the requirement to undertake business continuity planning to standards equivalent to BS25999 for category 2 responders that own critical infrastructure.

2.50 The Programme will analyse the current status of responder business continuity and seek to improve adoption levels through best practice, rather than necessarily expecting organisations to seek formal accreditation.

Impact assessment

2.51 An impact assessment and new burdens assessment will be carried out throughout the policy development process to ensure the proposals are appropriate and proportionate to the risks. The options and proposals will be assessed, before making recommendations such that the impacts are identified, understood and mitigated where necessary.

2.52 The process also gives the opportunity for those potentially affected to understand and challenge:

- (a) why the government is proposing to intervene;
- (b) the potential impact of a policy; and
- (c) the estimated costs and benefits proposed.

It also provides opportunities to identify unintended consequences.

2.53 The final impact assessment will be published alongside the National Resilience Plan during its consultation phase in late 2010.

National Resilience Plan for Critical Infrastructure

2.54 The development of the National Resilience Plan for Critical Infrastructure will be rooted in a partnership between the many public and private sector bodies involved and infrastructure owners/operators. It will bring together evidence from this Framework, Sector Resilience Plans and relevant analysis to set out a long-term, all-risks programme to reduce the vulnerability of critical infrastructure and essential services to severe disruption from natural hazards. It will set out proportionate policies and standards, and the resilience-building programmes necessary to achieve them. In addition, it will set out the Government's expectations and guidance on good practice.

Timetable

2.55 The Government's response to the Pitt Review recommendations set a target date for the development of the first Sector Resilience Plans of 31 December 2009. This target date was achieved.

2.56 The National Resilience Plan for Infrastructure will be available in draft for consultation late 2010, and then published in 2011.

2.57 The Programme will focus on current risks that we face in the UK in line with the National Risk Register's 5 year planning horizon, and seek to improve resilience

accordingly. Future risks should be considered when taking action to build resilience to factor in allowance for climate change.

2.58 The delivery of measures to improve the resilience of critical infrastructure is partly dependent on regulatory review cycles (in the regulated sectors) and hence funding availability. The Government expects the regulators to make some funding available during price reviews for measures to improve resilience in the short term.

SECTION 3: POLICY AND STANDARDS

The Impact of Natural Hazards

3.1 The main types of flooding to be considered are:

- Rain leading to fluvial (river) flooding. This is mainly associated with prolonged and often widespread rainfall or from convective rainfall over a period of time. The chance of river flooding is higher where cells of heavy rain occur within a wider rain band, or if the ground is already saturated from earlier rain, or if combined with rapid snowmelt.
- Rain leading to 'flash' flooding. This often arises from heavy, localised thunderstorms, which are more likely to occur in the summer months due to the convective nature of the rainfall. The impacts can be serious localised flooding, particularly in urban areas.
- Coastal and Tidal flooding. Weather, principally wind, causes increased wave heights or a tidal surge which can result in the overtopping or breaching of sea defences.

3.2 Surface water and groundwater flooding are also important considerations and will be included within the resilience-building programme as fuller information on these risks becomes available from the agencies responsible for flooding.

3.3 The National Risk Register also identifies risks from other natural hazards relevant to the UK, including:

- Strong winds. Storm events (such as occurred in the UK in 1987, 1990, 1998, 2000, 2002, 2005 and 2007) bringing extreme winds are usually the greatest risk to life and property in this country and cause disruption to power, transport and communications.
- Snow. Most winters in the UK have at least one period of heavy snowfall bringing serious disruption to public services.
- Extremes of heat and cold. Increased mortality is a well-documented phenomenon when the temperature moves away from the optimum. During August 2003, France suffered 15,000 excess deaths as a direct result of unprecedentedly high day and night temperatures.¹ That said, the impact on critical infrastructure is less well understood.
- Dry spells. Long periods without significant rain lead not only to water resource problems but also forest fires, and building subsidence as clay soils dry out.

3.4 Most of the categories of severe weather described above can usually be forecast in the general sense, out to some days ahead. However, for many events, it is the fine detail of the forecast which is most vital. Thus, although heavy rain can be disruptive, it is the much smaller areas of extreme rainfall which are likely to generate the highest flood risk.

3.5 The levels of variability and uncertainty inherent in predicting the incidence and impact of natural hazards across the medium-term – and especially extreme and localised events - presents a key challenge to the development of suitable resilience standards. The UK Climate Projections will,

¹ Department of Health Heatwave Plan 2009
www.dh.gov.uk

however, provide a platform for analysing the incidence and impact of natural hazards, now and into the medium-term future. The Cabinet Office will work with the Department for Environment, Food and Rural Affairs (Defra), the Meteorological Office and others to understand the probability of certain climatic events, and the impacts that could be experienced by critical infrastructure, across the short- and medium-term. These scenarios will subsequently be compared with the events currently considered by the owners of critical infrastructure.

UK Climate Projections (UKCP09)

The UK Climate Projections (UKCP09), launched on 18 June 2009, describe how the climate of the UK might change during this century. UKCP09 attaches probabilities to different levels of future climate change, allowing users to consider the implications of uncertainties and risks.

UKCP09 provides projections of changes for a number of climate variables (such as average temperature and precipitation), for 25x25km grid squares and for administrative regions and river basins. There are also projections for marine regions around the UK and for different scenarios of greenhouse gas emissions.

Flood Resilience Standards

3.6 Flooding is the first hazard being covered by the Critical Infrastructure Resilience Programme as it is the highest climatic risk in the National Risk Register, and because information on flood risk is available in a form which is more readily usable. This is not intended, however, to exclude other natural hazards; where there are known and well-defined vulnerabilities to other natural

hazards, these will be taken into account in initial resilience-building activity.

3.7 The Pitt Review concluded that: “for the purposes of building resilience in the critical infrastructure, a minimum standard of 1 in 200 (0.5%) annual probability would be a proportionate starting point [for all forms of flooding]”.

3.8 Ministers agreed in June 2009 to adopt the Pitt Recommendation as a minimum interim standard of protection from flooding for critical national infrastructure across all sectors. This will enable discussion between government departments, regulators, other public bodies and critical infrastructure owners to gather the shared evidence base on:

- the scale of the activity necessary to improve the resilience of relevant infrastructure to this standard;
- the cost of doing so, and over what practical timeframe; and
- the impact on owners’ business models and customers’ bills.

The interim standard will be reviewed in light of the above evidence being set out in the Sector Resilience Plans.

3.9 The Programme will consider how this interim standard could be developed to set out expectations of levels of resilience of critical infrastructure in terms of continuity of service. A broader approach for resilience standards may consider the contribution from prevention, protection and preparedness towards overall resilience of infrastructure networks and systems. Each element may require guidance on expectations, for example standards of protection from flooding may continue to utilise the 1 in 200 (0.5%) annual probability event for national infrastructure, with perhaps a higher standard such as a 1 in 1000 (0.1%) annual probability

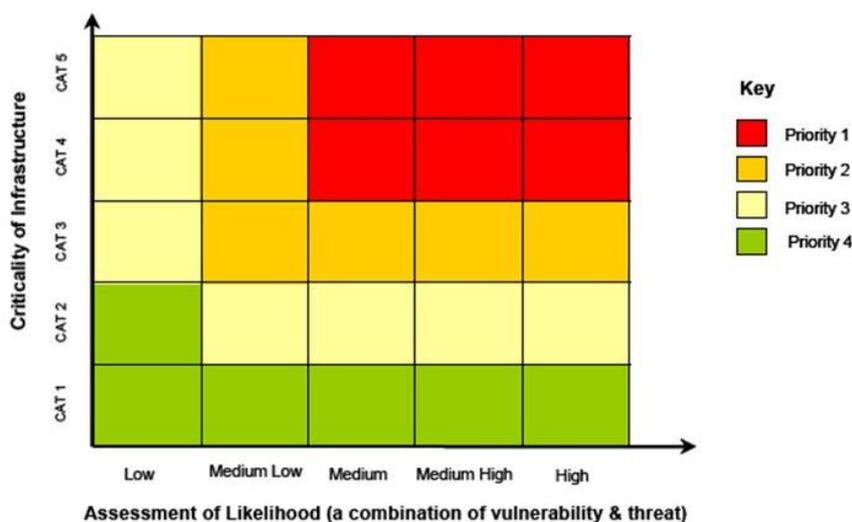
flood event for the most critical national infrastructure. The resilience standards should be flexible and take into account three risk factors:

- Probability of an event of a certain severity arising.
- Vulnerability of the infrastructure to harm from an event.
- Impact of the harm on the infrastructure as a result of the event, including the scale of the loss of service, the ability for the system to recover and the availability of alternative supplies.

3.10 The feasibility and merits of setting resilience standards will be examined using the evidence submitted in response to the consultation on the earlier draft of this Framework, and follow-up consultation workshops. Where infrastructure owners and regulators are already considering measures to improve the resilience of the most critical infrastructure, they are encouraged to adopt higher standards of protection in circumstances where the costs and benefits justify the additional investment.

3.11 It will remain for owners of critical infrastructure and providers of essential services to assess the vulnerability and impact of flooding on their assets and services to severe flooding, drawing on information available from the Environment Agency. The grid in figure 2 below is offered as a simple model to assist in prioritising assets where resilience-building actions are required. As a minimum, priority 1 sites must be covered within the first Sector Resilience Plans. Other priority sites should be included in annual reviews and updates of Sector Resilience Plans.

Figure 2: Using a Risk-Based Approach to Prioritise Sector Resilience Planning



SECTION 4: ROLES AND RESPONSIBILITIES

4.1 This section describes the roles and responsibilities of those organisations with the most significant potential contribution to build resilience into the infrastructure networks and systems in the UK. There are many other organisations that have a vital role in planning, preparing for, detecting, responding to and recovering from incidents associated with natural hazards. Their views and input will be sought to ensure the success of the Critical Infrastructure Resilience Programme.

Cabinet Office

4.2 The Cabinet Office is charged with developing the cross-sector resilience-building programme, with a clear remit to work across government departments and other public and private sector bodies to define and deliver shared goals.

4.3 The Cabinet Office also provides secretariat support to Cabinet Committees, including MISC36 to which this Programme reports.

4.4 The senior responsible owner (SRO) for this Programme within government is the Director of the Civil Contingencies Secretariat. The SRO is responsible for monitoring and managing the cross-sector effort to achieve the outcomes sought from the Programme.

Government Departments

4.5 Sponsoring government departments are responsible for working with regulators and relevant infrastructure operators and providers of essential services to determine the overall approach to be adopted within their sectors. Within this, key responsibilities include:

- Identifying what infrastructure within their sectors may be considered to be at risk of severe disruption from defined natural hazards, and the criticality of that infrastructure.
- Developing Sector Resilience Plans with the owners of critical infrastructure.
- Agreeing appropriate priorities and programmes of measures to improve resilience (as part of the Sector Resilience Plans) with critical infrastructure owners and regulators.
- Monitoring and reporting on activity and progress in their sector.
- Working with regulators (where they exist) to ensure the delivery of agreed programmes of resilience-building, including intervention in cases where infrastructure owners fail to implement agreed and funded programmes.
- Leading on any funding or regulatory issues that arise.

4.6 Infrastructure UK has been established in the Treasury to improve long-term planning and prioritisation of infrastructure, enabling investment and improving delivery. This includes consideration of resilience issues. A strategy for national infrastructure will be published at Budget 2010.

Devolved Administrations

4.7 The Devolved Administrations are the Welsh Assembly Government as the executive for the National Assembly for Wales, the Northern Ireland Executive for the Northern Ireland Assembly and the Scottish Executive for the Scottish Parliament. The Programme is being developed in consultation with the Devolved Administrations with the aim of delivering the same outcomes in terms of resilience of critical infrastructure across the UK.

4.8 The National Assembly for Wales has powers to legislate on matters such as fire and rescue services, food, highways and transport, water, spatial planning and local government.

4.9 The Northern Ireland Assembly has legislative competence over transferred matters, defined as all those that are neither excepted nor reserved. Excepted issues include national security and nuclear energy. Reserved matters include broadcasting. Transferred matters include social security, housing, economic development, local government, environmental issues, planning, and transport.

4.10 The Scottish Parliament has the power to pass primary legislation in respect of devolved matters, but cannot legislate on reserved matters. Reserved matters include the Civil Service, aspects of energy regulation (e.g. electricity, coal, oil and gas and nuclear energy), aspects of transport (e.g. regulation of air services, rail and international shipping) and broadcasting. Devolved matters include education, Local Government, housing and policing. The Scottish Executive has established a Strategic CNI Group to address all issues impacting on devolved matters relating to CNI in Scotland. This work has been endorsed by the UK Government and seeks

to adopt a holistic approach to the CNI, working in partnership with UK Government departments.

Regulators

4.11 The Pitt Review considered that “regulators should be given an explicit duty to take resilience into account, along with guidance to ensure clarity and that it is given appropriate regard.”

4.12 The regulators are vital to the analysis of gaps in the current system of regulation, and on how the system may need to change to support increasing the reserve capacity of supply.

4.13 The health sector, as well as the emergency services sector and part of the transport sector, are not regulated in the same way as the water and energy sectors. A different approach will thus be needed with those sectors to deliver the aims of this Programme.

Infrastructure Owners and Operators

4.14 Infrastructure owners and operators are established businesses operating in very different markets, which are often highly competitive. These businesses have various mechanisms and procedures to ensure the effective provision of their services to customers and to maintain (through market forces and regulation) a level of resilience within their infrastructure.

4.15 The Civil Contingencies Act 2004 provides the principal legislative framework for risk mitigation, preparedness and emergency planning. Many of the owners of critical infrastructure and providers of essential services are designated as either

Category 1 or Category 2 responders under the Act. The utilities (excepting electricity generators) are Category 2 responders and the Act places general duties on them to cooperate and to share information with Category 1 responders (mainly the emergency services and local authorities). This enables Category 1 responders to undertake community risk assessments and local contingency planning duties.

4.16 Specific legislation for infrastructure sectors contains complementary provisions to plan for, prevent and respond to threats. However, there is not widespread consistency across sectors in the process or standards adopted for building resilience. In addition, Sir Michael Pitt's report described the way in which the priority given to the mitigation of natural hazards varies within and between sectors.

4.17 Through working in partnership with regulators and government departments within the context of this Programme, infrastructure owners and operators will be encouraged to take forward the building of greater and more consistent levels of resilience in critical infrastructure to severe disruption from natural hazards.

Centre for the Protection of National Infrastructure (CPNI)

4.18 CPNI is the Government authority for protective security advice to the national infrastructure relating to national security threats. It comprises teams of expert advisers

who conduct security reviews and provides advice across the nine national infrastructure sectors aimed at reducing vulnerability to these threats. These advisers are supported by experts who undertake research and horizon scanning.

Environment Agency

4.19 The Environment Agency regulates air, land and water across England and Wales, and has responsibilities for flood and coastal erosion risk management.

4.20 The Environment Agency provides advice and information on flood risk and environmental matters, including publishing flood risk maps and data on the internet to raise public awareness and to support spatial planning. It also provides flood forecasting and warning services, maintains rivers and flood defences, and constructs new flood defences where necessary.

ANNEX A

Categorising infrastructure and the criticality scale

A1.1 The nine national infrastructure sectors are further broken down into sub-sectors. These are set out below.

Table A1: The nine national infrastructure sectors with associated sub sectors

National Infrastructure Sector	Sub Sector	Whitehall Sector Sponsor Dept	Lead in Scotland	Lead in Wales	Lead in Northern Ireland
Communications	-Telecommunications	BIS	BIS	BIS	NIO
	-Postal Services	BIS	BIS	BIS	
	-Broadcast	DCMS	DCMS	DCMS	
Emergency Services	-Ambulance	DH	SE	WAG	NIO
	-Fire & Rescue	DCLG	SE	WAG	NIO
	-Marine	DfT	DfT	DfT	NIO
	-Police	HO	SE	HO & WAG	NIO
Energy	-Electricity	DECC	DECC	DECC	NIO
	-Gas				
	-Fuel				
Finance	-Payment, Clearing & Settlement Systems	HMT	HMT	HMT	NIO
	-Markets & Exchanges	HMT	HMT	HMT	NIO
	-Public Finances	HMT	HMT	HMT	NIO
Food	-Production	DEFRA & FSA	SE	WAG & FSA	NIO
	-Processing				
	-Import				
	-Distribution				
	-Retail				
Government	-Central government ²	CO			NIO
	-Devolved Administrations/Functions;		SE	WAG	NIO
	-Regional & Local government;	CLG	SE	WAG	NIO
	-Parliament	Palace of Westminster Authorities ³	Scottish Parliamentary		
Health	-Health & Social Care	DH	SE	WAG	NIO
Transport	-Aviation	DfT	DfT	DfT	DfT/NIO
	-Maritime	DfT	DfT	DfT	DfT/NIO
	-Land	DfT,	SE(road)	WAG(road)	NIO (road+ rail)
Water	-Potable Water Supply	DEFRA	SE	WAG	NIO
	-Waste Water Services				
	-Dams				

Key

BIS: Department for Business, Innovation and Skills, **CLG:** Department for Communities and Local Government, **CO:** Cabinet Office, **DCMS:** Department for Culture, Media and Sport, **DECC:** Department of Energy and Climate Change, **Defra:** Department for Environment, Food and Rural Affairs, **DfT:** Department for Transport, **DH:** Department of Health, **FSA:** Food Standards Agency, **HO:** Home Office, **HMT:** Her Majesty's Treasury, **NIO:** Northern Ireland Office, **SE:** Scottish Executive, **WAG:** Welsh Assembly Government.

² And reserved functions thereof such as Defence and National Security.

³ Although not a Whitehall government department, these authorities lead on the security of Parliament.

A1.2 Infrastructure is categorised according to its value or “criticality” and the impact of its loss. This categorisation is done using the Government “Criticality Scale”, which assigns categories for different degrees of severity of impact. Table A2 provides broad descriptions of the sorts of types of infrastructure that would be categorised at the different levels (more detailed and specific impact criteria for each sector is captured in the Scale). For example, Category 5 (CAT 5) indicates infrastructure which would have the most severe impact when it is disrupted; CAT 0 indicates infrastructure whose loss would be minimal when considered in the national context.

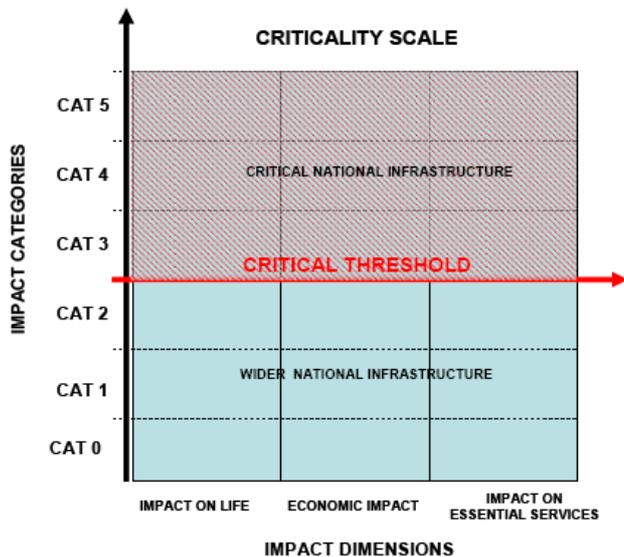
A1.3 Not everything within a national infrastructure sector is “critical”. Within the sectors there are certain “critical” elements of infrastructure, the loss or compromise of which would have a major detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life. These “critical” assets make up the nation’s Critical National Infrastructure (CNI) and are referred to individually as “infrastructure assets”. Infrastructure assets may be physical (e.g. sites, installations, pieces of equipment) or logical (e.g. information networks, systems).

A1.4 The Criticality Scale includes three impact dimensions: impact on delivery of the nation’s essential services; economic impact (arising from loss of essential service) and impact on life (arising from loss of essential service). These are illustrated in figure A1. Infrastructure may be classified using any one of these factors of impact. The designation should reflect the highest criticality category reached in either of the impact dimensions.

Table A2: Criticality Scale for national infrastructure

Criticality Scale	Description
CAT 5	This is infrastructure the loss of which would have a catastrophic impact on the UK. These assets will be of unique national importance whose loss would have national long-term effects and may impact across a number of sectors. Relatively few are expected to meet the Cat 5 criteria
CAT 4	Infrastructure of the highest importance to the sectors should fall within this category. The impact of loss of these assets on essential services would be severe and may impact provision of essential services across the UK or to millions of citizens
CAT 3	Infrastructure of substantial importance to the sectors and the delivery of essential services, the loss of which could affect a large geographic region or many hundreds of thousands of people
CAT 2	Infrastructure whose loss would have a significant impact on the delivery of essential services leading to loss, or disruption, of service to tens of thousands of people or affecting whole counties or equivalents
CAT 1	Infrastructure whose loss could cause moderate disruption to service delivery, most likely on a localised basis and affecting thousands of citizens
CAT 0	Infrastructure the impact of the loss of which would be minor (on national scale).

Figure A1: The three dimensions of the criticality scale



essential service impact criteria (criticality criteria) for their sector. The Natural Hazards Team will work closely with sponsor departments and CPNI to ensure that the interconnectivity of essential services is considered to enable an assessment of the risks from natural hazards.

A1.5 The following three factors provide the means to distinguish between different degrees of severity of impact on essential services:

- The degree of disruption to an essential service
- The extent of the disruption, in terms of population impacted or geographical spread
- The length of time the disruption persists.

A1.6 A critical threshold has been set on the scale and is the level above which the impacts of loss are considered so severe that infrastructure falling into these categories should be considered to form part of the Critical National Infrastructure. The threshold is currently set at CAT 3.

A1.7 Sponsor departments (and the Devolved Administrations) lead on identifying what infrastructure in their sector may be considered critical, in conjunction with sector experts at the Centre for the Protection of National Infrastructure (CPNI). Sponsor departments also lead on setting the