CabinetOffice

A Summary of the:

Sector Resilience Plans for Critical Infrastructure 2010 / 2011

May 2011

Produced by:

Cabinet Office
22 Whitehall
LONDON
SW1A 2WH

www.cabinetoffice.gov.uk

Contact:

Civil Contingencies Secretariat

naturalhazards@cabinet-office.x.gsi.gov.uk

Publication date: May 2011

Contents

INTRODUCTION

The Cumbria floods in 2009, the 'Big Freeze' of 2009 and 2010 and the eruption of the Eyjafjallajokull volcano in Iceland all highlighted the vulnerability of the UK's infrastructure to disruption from natural hazards. The worst disruption in recent times was as a consequence of the summer floods of 2007, and the impact that these had on elements of critical infrastructure - 350,000 people were without drinking water for up to 17 days and tens of thousands of people without power or stranded on road and rail networks.

The National Security Strategy[1] and Strategic Defence and Security Review[2] recognised the risk from natural disasters as one of the top tier risks facing the UK, and made the continued provision of essential services in such circumstances as one of the Government's resilience priorities.

In support of the National Security Strategy and the Strategic Defence and Security Review, the Critical Infrastructure Resilience Programme, led by the Cabinet Office, is developing a systematic, coordinated, cross-sector campaign to reduce the disruption caused by natural hazards to the UK's critical infrastructure.

A key output from this programme are the Sector Resilience Plans, developed by lead government departments for the nine national infrastructure sectors[3] setting out the current level of resilience of critical infrastructure to natural hazards.

Each Sector Plan is produced on an annual basis (the first plans were produced in 2009/2010), and placed before Ministers for information to assist them in their sector oversight role.

The Plans alert Ministers to any perceived vulnerabilities and set out a programme of measures to improve resilience where necessary.

Owing to the sensitive nature of the individual plans, distribution is limited to the Sector's Lead Minister, the Cabinet Office (Civil Contingencies Secretariat), and the Centre for the Protection of National Infrastructure.

This document presents an unclassified summary of those Plans.

Scope

While this Summary has been prepared with a UK wide focus, it is important to note that separate arrangements are in place within the Devolved Administrations, where in terms of the Devolution Settlements, the resilience of certain sectors is fully devolved. The Devolved

[1,2] www.cabinetoffice.gov.uk/content/national-security-council

[3] The National Infrastructure is categorised into nine sectors: Water, Energy, Transport, Communications, Health, Emergency Services, Finance, Food and Government. Some sectors are further divided into sub-sectors, as represented in Figure 1

Administrations are fully engaged in the Critical Infrastructure Resilience Programme and have arrangements in place to assess the resilience of the devolved sectors in each of their respective areas. For example, in Scotland, the water, transport (roads), health, emergency services, food and government sectors have all prepared Sector Resilience Assessments, which complement the Sector Resilience Plans prepared for those sectors in England.

The 2010 /11 Sector Resilience Plans presents a snapshot of the resilience of the UK's critical infrastructure to disruption from natural hazards as at the end of the first quarter of 2011.

National Infrastructure

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".

Within the national infrastructure, there are certain critical elements, the loss or compromise of which would have a major impact on the availability or integrity of essential services leading to severe economic or social consequences or to loss of life in the UK. These critical elements make up the critical national infrastructure (CNI).

Figure 1 shows the nine national infrastructure sectors and associated sub-sectors.

Resilience

In the Critical Infrastructure Resilience Programme, resilience is defined as "the ability of a system or organisation to withstand and recover from adversity".

A resilient organisation is one that is still able to achieve its core objectives in the face of adversity through a combination of measures.

Physical protection may make up an important part of resilience, but it is not the only factor. Resilience is also underpinned by good design of infrastructure networks, effective emergency response, business continuity planning, and recovery arrangements.

2010 / 11 Sector Resilience Plan

To share best practice and promote cross sector resilience building, the Cabinet Office produces an unclassified summary of the annual sector plans. It provides a concise snapshot of each sector's resilience to natural hazards and outlines the approach sectors will take to improve the current level of resilience.

The first iteration of the Sector Resilience Plans, completed in January 2010, reported on the resilience of CNI assets in each sector to coastal and fluvial flooding.[4] Some departments also reported on the generic resilience in their sector, exercise programmes, business continuity planning and ongoing work with industry and regulators to build resilience to flooding.

The scope of the 2010/11 Sector Resilience Plans has been expanded to provide Lead Government Departments the flexibility to consider the resilience of their infrastructure (including, where appropriate, less critical infrastructure or network resilience) to the natural hazards most likely to cause disruption.

One natural hazard of particular interest to the infrastructure sectors is severe space weather (solar activity that can affect the performance of both space and ground infrastructure). This phenomenon is known to particularly affect the electricity and telecommunications (particularly in relation to satellite communications) sub sectors, consequently affecting all other sectors. This is a complex area of work where the Government is working closely with industry and the scientific community to assess its impact on the delivery of essential services, the findings of which will be used to inform cross sector planning.

Dependencies

Throughout this summary, references are made to the dependency one sector may have on another, for example, the importance of communications to the finance sector. As a consequence of these dependencies between sectors, there is a risk that a minor disruption in one sector may result in a major disruption in another sector.

As the Sector Resilience Plans continue to develop, these dependencies are beginning to be understood. However, the size and complexity of the infrastructure networks and systems across the UK mean that a complete understanding of the dependencies and interdependencies is not realistically achievable across every system. However, bringing organisations together will enable discussion about the major installations and infrastructure networks that supply essential services to communities within a region.

To assist with this process, practical guidance has been developed to enable emergency responders and infrastructure owners and operators to work together and develop a sufficient understanding of infrastructure networks and dependencies across sectors.[5]

Next Steps

The Sector Resilience Plans are an essential part of the Critical Infrastructure Resilience Programme.

[4] www.cabinetoffice.gov.uk/infrastructure-resilience

The Plans report on the current level of resilience within each sector and set out a programme of measures to address vulnerabilities. The Critical Infrastructure Resilience Programme will oversee delivery of these actions to improve resilience.

Details of the Programme can be found in the Guide, '*Keeping the Country Running: Natural Hazards and Infrastructure*',[5] which provides guidance for regulators, infrastructure owners/operators and emergency responders on building resilience in infrastructure.

The Programme will continue to have close links with (a) Infrastructure UK (IUK), which is focusing on the UK's long-term infrastructure priorities,[6] and (b) the Government's Adapting to Climate Change Programme, which takes a broader view of how future climate will impact on an organisation's functions and how organisations will need to adapt to these impacts.[7] This programme recently published a report that outlines the long term challenges to the transport, energy, water and information and communication technology (ICT) infrastructure sectors to adapting to climate change.[8]

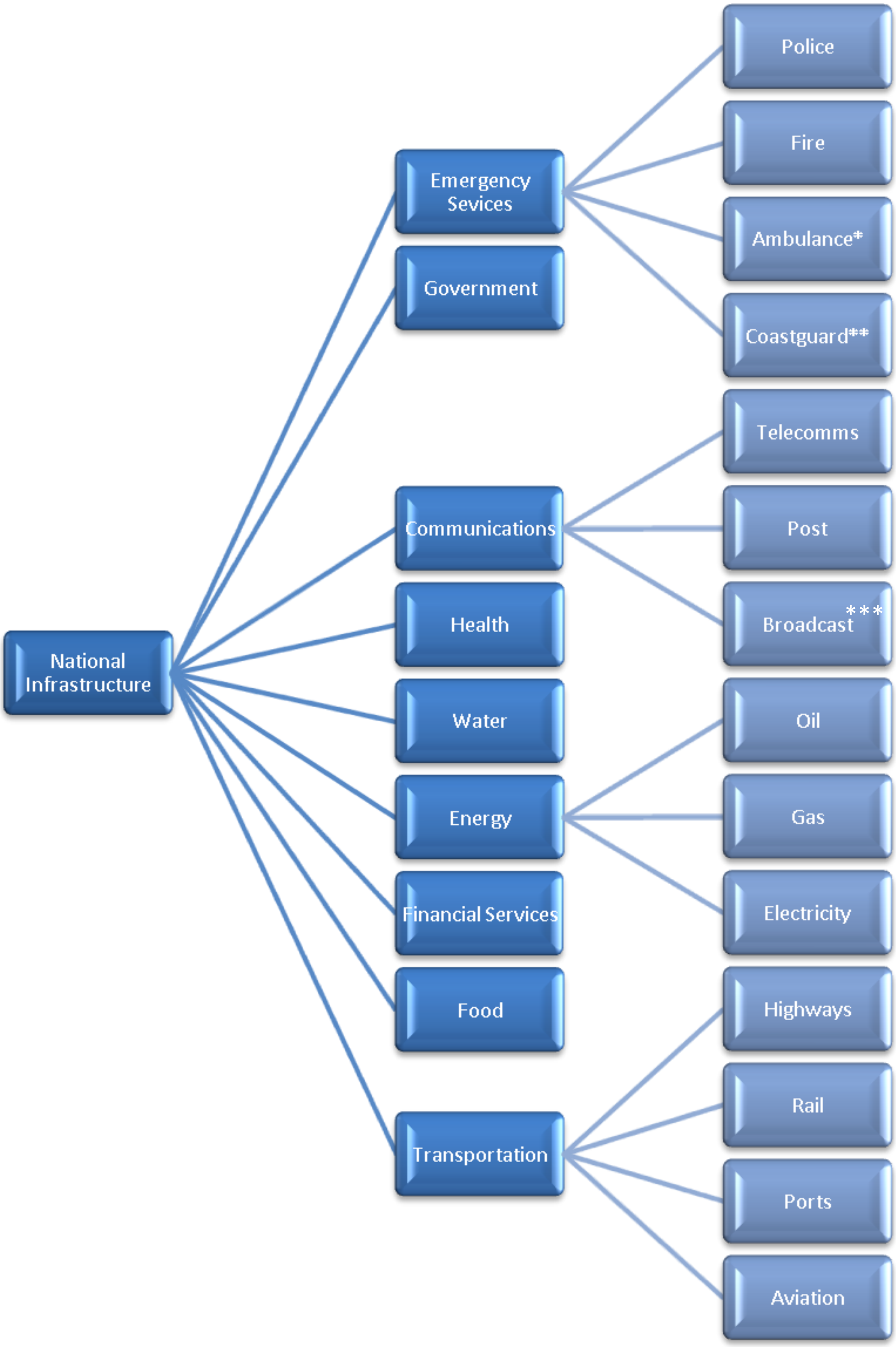
[5] www.cabinetoffice.gov.uk/infrastructure-resilience

[6] The Strategy for National Infrastructure and details on Infrastructure UK can be found at: www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_186451.pdf

[7] Further information on the Adapting to Climate Change Programme can be found at: www.defra.gov.uk

[8] www.defra.gov.uk/environment/climate/sectors/infrastructure-companies/

Figure 1: The nine national infrastructure sectors with associated sub-sectors



* Ambulance sub-sector is managed as part of the health sector

**Coastguard sub-sector is managed as part of the transport sector

*** Broadcast to be included in 2011/12 Plan

ENERGY

Overview

Natural hazards continue to pose a risk to the uninterrupted supply of energy to the UK, but Government and industry led programmes are in place to ensure that the risk of disruption is continuously reducing.

Sector Approach

The Energy sector is made up of three sub sectors: Electricity, Gas and Oil. As sponsor department for the sector, the Department of Energy and Climate Change (DECC) has reviewed the quality of each sub-sector's resilience to pandemic influenza, flooding, heat wave, drought and storms. DECC has also outlined the programmes currently underway or committed that will enhance the resilience of its infrastructure.

Assessment of Existing Vulnerability

The energy sector has robust procedures in place to identify, evaluate and reduce the risk from natural hazards to infrastructure. DECC works with industry and regulators to continually review and enhance the resilience of its infrastructure, where necessary and proportionate.

Dependent on the nature of the sub-sector, the sector's level of resilience can be maintained / enhanced through regulation, legislation and licensing measures; price control reviews and investment; design and service standards; guidance; and robust contingency arrangements. For example:

- Guaranteed Standards of Service: under the Utilities Act 2002, Ofgem introduced performance levels for the gas and electricity industry e.g. supply restoration timescales and investigating complaints about voltage levels within agreed timescales.

- The electricity network companies have worked together with Ofgem, under the auspices of the Energy Networks Association, to produce an Engineering Technical Report "Resilience to Flooding of Grid and Primary Substations" (ETR138). The purpose of ETR138 is to present a risk based methodology that provides guidance on how to improve the resilience of electricity substations to flooding to a level that is acceptable to customers, Ofgem and Government, taking account of a cost/benefit assessment for each site.

- While overhead lines and underground cables are resilient to flooding, the former are susceptible to damage from strong winds, which bring trees and windborne debris into contact with overhead lines. To reduce the risk from vegetation, a new regulation came into force in 2009. The Electricity Safety, Quality and Continuity Regulations

(ESQCR) requires that a generator or distributor shall, so far as is reasonably practicable, ensure that there is no interference with or interruption of supply caused by an insufficient clearance between overhead lines and trees.

- Upstream Oil and Gas infrastructure is subject to ‘permissioning’ regimes for the purposes of health and safety. These are applied through the Offshore Safety Case Regulations, the Pipelines Safety Regulations, and the Control of Major Accident Hazards (COMAH) regulations for onshore facilities. These regimes provide for a review of the design basis for facilities in the event of new or increased hazards, and provide an existing regulatory mechanism for dealing with changes in the risk profile.

Owing to the size and complexity of energy networks, completion of resilience building programmes can take a number of years, and until such programmes are complete, infrastructure remains exposed to (an ever decreasing risk of) disruption .

For example, the major substation sites at risk of flooding have been identified and a remedial work programme is in hand, focused initially onto those sites with the greatest risk. However, the work is not expected to be completed until 2022, and so there will be residual, reducing risk for the next twelve years.

In contrast to wind and flooding, the level of risk associated with pandemic influenza is beyond the control of the energy sector, which can only seek to mitigate its potential impact. The extensive work that was undertaken before and during the pandemic of 2009 supported the view that infection rates were unlikely to reach the point where the critical energy infrastructure could not be operated.

The main risks to service continuity are reduced staffing levels and supply chain disruption of critical products. Across the sector, organisations have in place contingency plans that would manage all but the most severe flu pandemic. During the 2009 H1N1 flu pandemic, monitoring of infection rates was introduced to give warning if rates should approach these levels. Contingency planning was undertaken for prioritising deliveries and relaxing regulatory requirements, should that have become necessary.

Building Resilience

The energy sector is committed to, where necessary, put in place proportionate measures to ensure the continued delivery of its services during periods of extreme weather.

Across the sector, programmes currently underway or committed to include:

Sector - Wide

- Further analysis of the impact of severe space weather on the energy sector;

- Assessment of the risk posed to the sector's critical supply chain from natural hazards and pandemics;

- Assessment of the risk to energy supply from surface water flooding.

Upstream Oil and Gas

- Assessment of the risk to oil and gas beach terminals from fluvial and coastal flooding

Electricity Generation

- Assessment of the risk to power stations from fluvial and coastal flooding;

- Identification of power stations at risk of having their service constrained by a shortage of cooling water;

Electricity Networks

- Completion of the electricity networks vegetation management programme;

- Assessment of the risk posed by severe space whether, which is known to affect electricity transmission networks.

DECC will continue to work with infrastructure owners, regulators and trade bodies to ensure that the sector continues to deliver improvements in the resilience of its infrastructure to disruption from natural hazards.

Background

The energy sector consists of electricity generation, transmission and distribution companies, gas distribution networks, gas transmission and upstream gas production, oil production, refining, supply and distribution.

Downstream oil, electricity generation and supply of gas/electricity are considered to be competitive markets and as a result they are not price regulated. The electricity and gas transmission and distribution networks are natural monopolies and are subject to price controls, which currently include a provision for investment in flood defences, and are regulated by the Office of the Gas and Electricity Markets (Ofgem).

COMMUNICATIONS

TELECOMS

Overview

The overlapping nature of telecommunications networks and historic investment in infrastructure in the sector, coupled with the work undertaken by the Department for Business, Innovation and Skills (BIS) with the UK telecoms industry, has enhanced the resilience of the sector's services to natural hazards.

Sector Approach

For the 2010 /11 Sector Resilience Plan, BIS has worked with industry to review the sector's generic contingency arrangements; its resilience to flooding and extreme cold with snow events; and dependencies with other national infrastructure sectors.

Assessment of Existing Vulnerability

The Electronic Communications – Resilience and Response Group (EC-RRG) has representatives from all of the major telecoms providers as well as relevant Government Departments and leads on maintaining resilience within the telecoms sector. The EC-RRG manages the Telecoms Emergency Plan, which sets out management processes for handling emergencies, priority customers and priority services.

Each individual telecoms operator has its own plans for how to manage an emergency affecting its systems as well as plans to restore services to customers.

Owing to the competitive nature of the sector, historic investment in the infrastructure and the range of alternative systems (e.g. land line, mobile, internet), the industry is inherently resilient. In addition, the industry has invested in infrastructure to avoid any large single points of failure. For example, all the major telecoms providers have back-up operation centres and switches have dual-routing or alternatives so telecoms traffic can be re-routed quickly and simply if one switch fails.

Also, companies have made options available should there be serious network problems in the UK, notably the additional capacity to re-route outside the UK.

The 2009/10 sector resilience plan focussed in detail on flooding. All of the assets at risk from flooding had back up facilities and tested contingency arrangements in place. Owing to reasons set out above, the sector is able to manage disruption from flooding in an effective manner.

Nevertheless, the EC-RRG has continued to focus on preparedness in this area including continuing to share good practice on flood preparedness and utilising data provided by the Environment Agency.

For other natural hazards:

- Recent events such as the 2009 flu pandemic and the 2010 volcanic ash event caused the sector very little disruption;

- More generally, the telecoms industry has to deal with problems caused by severe weather (including extreme cold with snow, flooding, and wind) conditions on a regular basis;

    - The most serious issue for the telecoms providers caused by severe cold, snow or flooding is the denial of access to affected sites. Where necessary, operators have deployable mobile equipment that can provide temporary back up until the site can be reached and repaired.
    - International design standards also aid mitigation, as most cables are designed to operate in extreme heat or cold (i.e. the same kit may be used in northern Finland as in Saudi Arabia); for this reason heat and drought are not considered an issue by operators.

The potential for infrastructure damage caused by snow, ice, high winds and lightning strikes, particularly in the Highlands and Islands of Western Scotland, is an ongoing problem that the telecoms providers have to address. These issues are normally classified as “business as usual” that the telecoms providers deal with on a regular basis. They are being addressed in the longer term by the increased use of fibre optic cabling, which is located underground and is therefore less susceptible to damage.

The sector is highly dependent on energy, for which it has built-in contingencies including back-up generation of at least 3 days’ duration independent of mains electricity grid at all telecoms critical national infrastructure sites and essential and emergency service key centres.

Building resilience

BIS is currently implementing the specific requirements under the European Electronic Communications Framework Directive. This is designed to enhance the security and resilience of communications networks and services and minimise disruption to them (legislation is due in May 2011).

The industry continues to invest to improve infrastructure and move towards more fibre optic use. International guidelines are followed in the design and maintenance of infrastructure.

BIS will continue to collaborate with industry to reduce any vulnerability to natural hazards through the work of EC-RRG, and increase the sector’s awareness of related risks, and produce annual sector resilience plans.

Under the requirements of the Digital Economy Act (DEA), Ofcom has an obligation to write every three years to the Secretary of State giving a full assessment of the UK's communications infrastructure, including its resilience. The first of these reports is due in Summer 2011.

Background

The UK telecoms industry is based around several different types of communication: fixed telephony, mobile telephony, and the internet and satellite communication.

BIS is responsible for ensuring the resilience of the telecommunications sector to the hazards and threats set out in the National Risk Assessment. To fulfil this role, BIS works in close partnership with the telecoms industry on the Electronic Communications – Resilience and Response Group (EC-RRG), which has representation from all of the UK's key telecoms companies including fixed and mobile operators and other service providers, as well as Government and Ofcom.

EC-RRG devises an annual work programme designed to enhance resilience in the telecoms sector. Work has included developing and sharing good practice on denial of access issues and improvement of the National Emergency Alert for Telecoms (NEAT). NEAT is convened in the event of an emergency where coordination is required between telecoms companies. It is used to coordinate an effective pan-industry response to restore normal service within the affected area as soon as possible (both on a service and a technical level).

The existing regulatory framework is a mixture of international, EU and UK regulation and industry self-regulation. Responding to the ever-changing threat from diverse sources and locations means the regulatory framework requires flexibility - as a consequence, the UK regulatory framework consists of self-regulation underpinned by supporting legislation.

The telecoms sector has traditionally been lightly regulated. The sector retains a very high level of availability of services (which are rarely disrupted). High levels of availability are required of the main 999 providers (BT, C&W and Kingston Communications). Other providers maintain high levels of resilience, and thus availability, because the market is extremely competitive and retaining customers is critical.

However while this record of resilience is very good, the forthcoming European Electronic Communications Framework Directive will require providers to ensure the security and resilience of their networks and services.

The Digital Economy Act 2010 sets out proposals that allow Ofcom to assess the delivery of communications services in the face of problems that are realistically likely to be faced and makes the promotion of investment in communications infrastructure one of Ofcom's principal duties.

POSTAL

Overview

The postal sector is considered to have a significant degree of resilience owing to the geographic spread of operations and the adaptability of the service in times of disruption.

Sector Approach

The 2010/11 Sector Resilience Plan reviewed the effectiveness of contingency arrangements against a range of natural hazards including flooding, storms and volcanic ash. The plan also set out where the industry is dependent on other sectors of national infrastructure.

Assessment of Vulnerability

Royal Mail's generic contingency plans respond in much the same way to a variety of interruptions/disruptions to services. In effect, the contingency plans work on the basis of diverting postal traffic around hot-spots (disrupted sites/operations). These plans are tested through local training and exercises and are put into practice on a regular basis in the face of various kinds of disruptions that affect the network (for example, local flooding and suspect packet incidents).
Royal Mail's Central Postal Control (based in central London with alternative arrangements in place outside London) monitors nationwide operations on a 24/7 basis and can quickly divert its fleet and postal traffic around any reported disruptions to roads or within its own network.

There are also alternative carriers (e.g. around 4,000 couriers in the UK) providing the sector with an additional layer of resilience.

In the case of natural hazards, Royal Mail can build in some protection at sites (and this is being addressed through local risk assessments), though for the most part major physical or structural changes to sites are unlikely to prove cost-effective. If local operations are affected by local flooding, Royal Mail has contingency plans in place to continue operations at alternative sites.

Transport is a critical dependency for the sector, particularly road and air transport. For example, heavy snow is likely to impact on Royal Mail's ability (and the abilities of other carriers) to move mail around the country (depending on the state of major routes – roads and airports) and to make collections and deliveries (depending on the local condition of roads and pavements).

There are local health and safety issues that Royal Mail must consider in determining whether it is safe to make local deliveries and collections and local risk assessments are often carried out for this purpose.

In those circumstances where local deliveries have been disrupted due to severe weather, contingency arrangements are introduced to recover any delays with mail that may have built up within the postal system.

International mail was badly affected by the disruption caused by volcanic ash in April 2010. Most UK postal and parcels operators were forced to divert mail from air to road services for main European destinations. This meant that postal traffic to Europe continued to flow, though these services were subject to delays.

Royal Mail introduced contingency arrangements to maintain international mail to destinations such as the US and Canada by trucking post to alternative European airports unaffected by the ash cloud and flown from those airports. Other carriers introduced similar measures to maintain their operations.

Electricity supply is also a key dependency, particularly with the use of mechanised sorting and other equipment, as well as IT systems. Royal Mail has a policy of providing standby generating plants for all major sorting offices, but this may not always allow for full operations and is dependent on the availability of fuel supplies.

Royal Mail also ensures that it maintains sufficient fuel stock at major sites and plans exist to build up fuel reserves in the event of intelligence of potential disruption to fuel supplies. Plans also exist to manage fuel reserves nationally.

In the event of an interruption of access to fuel, Royal Mail would allocate its resources in order to provide services in accordance with corporate priorities that have been reviewed by Postcomm, the industry regulator.

Building Resilience

As the sole universal service provider with its network as the core of the UK postal services sector, Royal Mail is obliged by licence condition to maintain robust contingency plans. The company's primary objective is to maintain services and that means in those cases where there is a specific risk of disruption of operations e.g. flooding, some physical protective measures may be considered. In most cases, robust contingency plans ensure that work is diverted around the disrupted unit, thus maintaining services.

BIS will continue to liaise with Royal Mail, other operators and the regulator on an ongoing basis to ensure that hazards and threats to the sector are given appropriate consideration and proportionate measures are introduced wherever practicable to mitigate the associated risks.

Background

Royal Mail delivers 99% of letters in the UK and although other operators have picked up a proportion of the bulk mail market, these operators still rely heavily on Royal Mail's network for end delivery.   Royal Mail's network is a nationwide network of distribution hubs, sorting centres and delivery offices carrying out essentially the same operations. As a result, the system has a significant degree of resilience built into its operations, as postal traffic can be diverted around any particular disrupted unit with relative ease. This happens quite regularly within the postal system.

The criticality of Royal Mail's operations lies in the network infrastructure as a whole and not in specific operations/sites. Royal Mail's infrastructure involves around 115,000 pillar boxes, 12,000 post offices, and around 87,000 business addresses (collections). The network which shifts around 68 million items each day involves over 60 mail centres with a number of satellite collection hubs, 8 distribution centres, and around 1,400 delivery offices. Over 150,000 staff are involved in its operations. The mail is moved around the country by a fleet of around 30,000 vehicles.

Postal services were fully liberalised in January 2006 (the parcels and courier markets were opened up to competition in 1981), so there is a range of alternative carriers in the market. These carriers would only have the capability to deliver time critical mail and parcels. They would not be able to replicate Royal Mail's universal service.

Royal Mail is regulated by Postcomm, who require it to review its contingency plans every two years. Postcomm can at that time choose to object to the plan. Royal Mail can accept the objection or choose not to but has to give an explanation.

In October 2010, the Government announced a new Postal Services Bill, which among other things will allow for the privatisation of Royal Mail and the replacement of the existing licensing regime under Postcomm with a regulatory system based on general authorisation under the supervision of Ofcom.

WATER

Overview

The integration of resilience into the water sector's price review cycle has enabled the industry to enhance the resilience of its assets and strengthen contingency measures to disruption from natural hazards.

Sector approach

The Department for Environment, Food and Rural Affairs (Defra) is responsible for providing the strategic policy direction and statutory framework for the water sector wholly or mainly in England.   Defra and the Welsh Government has worked with industry and the Water Services Regulation Authority (Ofwat) to review the level of resilience to flooding, extreme cold with snow, pandemic flu and to the loss of power, communications and disruption to essential supply chains in England and Wales. In Scotland, the sector has prepared a separate Sector Resilience Assessment.

Assessment of existing vulnerability

The water industry is dependent on a supply of energy, telecoms and chemicals in order to function so the loss of any of these will potentially have an impact on the ability of water companies to deliver their service.

The loss of electricity causes pumping stations for drinking water to fail and can also disrupt the movement and treatment of sewage, although the impacts on sewage are less immediate as the majority of sewage movement is by gravity.

The main impact of a loss of communications would be on water companies' SCADA (Supervisory Control And Data Acquisition) systems. SCADA is an industrial computer system that controls and monitors the flow of sewage into and through a treatment works and monitors and controls the flow of treated water from a works into the network. It also monitors and records water quality data.

Loss of SCADA functions could ultimately result in the inability to stop the flow of sewage heading towards a treatment works. Therefore it may be necessary to discharge raw sewage onto land or into water courses.

Where SCADA was lost, sites would continue to run on the last known rate/output and water companies are able to sustain supplies through reversion to manual operation – through site visits on a fixed cycle to ensure that they are still functioning and to check levels, check processes and make the adjustments that would be normally done remotely.

While water companies have plans in place to manage and respond to the consequences of both a loss of SCADA and a loss of power for certain durations, no specific plans exist for severe space weather.

The timescales and cost of achieving improvements in understanding and resilience to this hazard across the industry are currently unknown as Defra is awaiting a detailed response from DECC and BIS on the impacts on telecoms and the national grid before proceeding.

During the snow in January 2010 the national shortage of salt and grit and the subsequent rationing and the prioritisation of major roads by local authorities led to potential water supply and water quality issues as access roads to a number of water treatment works were not gritted / impassable and delivery vehicles were unable to make deliveries of essential supplies of chemicals.

In the event of an incident, the Security and Emergency Measures Direction 1998,[9] under the provisions of Section 208 of the Water Industry Act 1991,[10] requires water and sewerage undertakers to "make, keep under review and revise such plans as it considers necessary to ensure the provision of essential water supply or, as the case may be, sewerage services at all times, including a civil emergency or any event threatening national security..." and under the requirement all water companies are to have plans that can be adapted to suit a variety of scenarios.

In 2004 the Water UK Council established a mutual aid protocol for all members to ensure delivery of water by companies in an emergency. Although water is a devolved issue the Water UK protocol was adopted across the UK. Across the industry stockpiles of emergency equipment held by the various companies are considerable and many companies have benefited from inter-company borrowing of such emergency equipment to supplement their own stocks during severe incidents.

Alternative water supplies would be provided through bottled water and bowsers in the street to those who were without mains water.

Building resilience

Defra has provided guidance to Ofwat to allow the cost of resilience to be met. This guidance will be kept under review to ensure that it allows companies (and Ofwat) to develop proportionate resilience measures.

Measures to further improve resilience will be developed jointly through a relationship between Defra, the Welsh Government, Ofwat and the water industry as the owners and operators of the assets.

Ofwat's final determination on water company prices in November 2009 provided for some £400m of

[9] www.cabinetoffice.gov.uk/media/132943/semd98.pdf
[10] www.legislation.gov.uk/ukpga/1991/56/section/208

expenditure by water companies over the next five years on making their treatment works and other assets more resilient to flooding and other hazards, thus protecting customer supply.

For additional work to be carried out during the period 2010-2015, providing Ofwat agree, the cost of this work will be 'logged up'. This is the process by which additional costs incurred between periodic reviews are taken into account at the next periodic review.

The SEMD requirements for each company are independently audited every year by Defra appointed Certifiers.

Ofwat's final determination on water company prices also provided for £400m to be spent on meeting SEMD requirements. SEMD covers all scales and types of incident. However, a particular focus is the provision of alternative water to large numbers of people should the piped supply fail.

Following the loss of Mythe water treatment works in the 2007 floods, and in response to recommendation 40 by Sir Michael Pitt,[11] SEMD was strengthened in 2009 in England and 2011 in Wales and the amount of alternative water to be provided should the piped supply fail was increased from 10 litres per person per day to 20 litres per person per day after 5 days.

Capability analysis is undertaken for the water industry twice a year and this enables long term capability targets to be set based on an assessment of the capabilities already in place against those required to cope with the risks in the National Risk Assessment. This process is coordinated by the Cabinet Office. Capability analysis looks at a range of scenarios that could disrupt water supply and sewerage services including the loss of infrastructure as a result of flooding, loss of electricity supply, loss of SCADA and loss of telecoms.

This analysis feeds into a balance of investment process as part of the next review of water price limits, taking into account any agreed long term delivery priorities. This delivery plan identifies the priorities for delivery until the process is complete.

As part of action being undertaken to improve long term resilience as part of climate change, water companies also produce Water Resource Management Plans[12] and Drought Plans[13] in order to ensure the provision of water supply.

As a result of the problems encountered in January 2010 a number of companies have increased their own stocks of grit and salt in order to ensure they can mitigate the effects of any rationing by local

[11] http://webarchive.nationalarchives.gov.uk/20100807034701/http://archive.cabinetoffice.gov.uk/pittreview/thepittreview/final_report.html

[12] *www.defra.gov.uk/environment/quality/water/resources/planning/*

[13] *www.defra.gov.uk/environment/quality/water/resources/drought/*

authorities as occurred during the snow.

Water companies have contingency plans in place which include the use of in-situ and mobile generators for key water treatment and sewage installations. In the event of a loss of power, back-up generators that are in situ at treatment works and pumping stations would take over but at reduced power.

Background

The UK water sector comprises a combination of private companies delivering water and sewerage services and public bodies which regulate drinking water quality and ensure companies provide household and business customers with value for money.

Water is a devolved issue with separate legislation for England, Wales and Scotland.

TRANSPORT

Overview

The variety of options provided by the UK's transport infrastructure makes the sector inherently resilient at the strategic level, although local disruption and inconvenience may result when people and businesses have to find alternatives to their preferred travel option. For the transport sector, ensuring safety and security for the public at large and transport users in particular must be a very strong focus. This can weigh against convenience when the system is under pressure.

Given the inherent resilience provided by multiple travel options, and the desire to avoid prohibitive pricing of travel, transport operators have made strategic decisions not to undertake every possible resilience measure, but instead to accept that, disruptive events outside normal parameters may cause temporary interruption of a proportion of services.

During the disruption and immediately afterwards the aim would be to maintain and then restore services to the greatest extent possible, subject to balancing safety considerations.

Sector Approach

The Department for Transport (DfT) is the Lead Government Department for the transport sector, which comprises the UK's roads, rail (including the Channel Tunnel), aviation and maritime/ports sectors. During 2010, elements of the transport sector were for short periods badly disrupted by volcanic ash and severe winter weather. The 2010/11 Transport Sector plan has therefore focussed on these two natural hazards.

Assessment of Existing Vulnerability

All transport services are either in the private sector or provided within the public sector at arms length from Government (e.g. Transport for London). The Government therefore has limited powers over the management of transport services. However it is in the transport operators' own commercial interest to plan for meeting disruptive challenges.

As the majority of sector regulators focus on safety and security; emergency planning remains the responsibility of transport operators. All will have business continuity plans covering the main risks to their operations. The focus of the Department for Transport is on monitoring and maintaining an overview of the sector's resilience at a strategic level, through being aware of each transport mode's contingency planning to mitigate key risks.

Owing to its structure and varied nature, it has an in-built overall resilience but can be affected at a local level across all sub-sectors. For this reason, cancellations of a proportion of operations tend to be more cost effective than trying to build in protective measures to the most extreme occurrences of natural hazards across whole networks.

During April 2010, the eruption of the Eyjafjallajokull volcano and the subsequent spread over mainland Europe of enormous amounts of volcanic ash caused the prolonged closure of UK airspace and severe disruption to the aviation industry. The European Union estimated that the cost of airspace closures across Europe was over £3bn.

Both during and since the eruption, DFT and the UK Civil Aviation Authority (CAA) have worked closely with the Met Office, the aviation industry, and European and international authorities to establish and agree a threshold of ash density that aircraft could tolerate safely, and therefore, continue to operate.

Following the severe weather experienced during the winters of 2008 / 09 and 2009 / 10 , the Department for Transport commissioned an independent review (the Winter Resilience Review), under the chairmanship of David Quarmby CBE, to identify practical measures to improve the response of the UK transport network.

The Winter Resilience Review published its interim findings in July 2010 and its final report in October 2010. The Government immediately accepted the Review's recommendations and as a result, the Department for Transport (DfT) is working with industry partners and regulators:

- In the short term, it has tasked the Highway Agency with building a national strategic reserve of 250,000 tonnes of salt. To bolster local supplies during periods of high demand. The majority of the reserve is now in place; and

- In the longer term, it is working with industry and the Local Government Association to:
    - improve resilience in salt supply through greater efficiencies in salt utilisation;
    - promote increased throughput flexibility by suppliers; and
    - ensure local highway authorities meet the new recommended standard of 12 days per season salt stocks.

In addition, since the Review DfT has:

- Worked with the UK Roads Liaison Group to produce guidance for local highway authorities on standards and methods to reduce the utilisation of salt without compromising effectiveness.

- Established an online portal for collecting data and monitoring salt levels and movements.

For all modes of transport the Review recommended that each should seek to improve its emergency communications during spells of extreme weather with the travelling public.

During the recent bout of severe winter weather (November 2010- January 2011), the Secretary of State for Transport commissioned David Quarmby to carry out a rapid audit of the response of the Highway Authorities and transport operators in England since the initial Winter Resilience Review.

The Audit found that “pretty well all the Recommendations we made in our main Review that could have been implemented by now have been, and that others with longer timescales are generally in process.” Response arrangements had therefore been strengthened in a number of key areas, notably salt usage and stockpiling. Local highway authorities reacted promptly to the unexpectedly harsh spell of cold weather by salting roads extensively and were then able to have depleted stocks replenished by release from the national strategic reserve.

Unlike the previous two winters, the rail network experienced severe disruption, particularly those networks south of the River Thames and in Scotland. The Audit recommended that the rail industry should conduct a strategic review of technical, more weather resilient alternatives, to the third rail / top contact system for the rail network south of the Thames. In Scotland, the Scottish Government is following up weather related resilience issues with Network Rail and other rail companies.

The snow also caused numerous flight cancellations and, at times, prolonged airport closures across the UK. The Government's South East Airports Task Force has been tasked with making recommendations about what more can be done to improve resilience in the aviation sector. The Government is also considering proposals, under a planned Bill to reform the economic regulation of airports, for a new licensing regime which would put increased focus on airports’ resilience to severe weather.

Building Resilience

DfT will continue to work with Transport industry partners to take forward the recommendations from the Winter Resilience Review, and those from the recent independent audit, of England’s response to the severe winter weather in 2010-2011. Similar work is being undertaken by the devolved administrations.

In addition DfT and CAA will continue to make an important contribution to international work to improve the resilience of the aviation industry to disruption from volcanic ash.

Background

The UK transport sector is dominated by private sector operations, with most regulation focussing on safety and security. The sector has a strong international focus and as such must comply with for example, European and international regulations, design and service standards.

The Department for Transport provides leadership across the sector to achieve its objectives. With regulators, it works to ensure compliance with industry specific regulations and standards. It works with regulators local, regional and private sector partners to ensure that the delivery of the UK’s transport services comply with national and international regulations, standards and meets the needs of the public and the wider society.

In Wales, the Welsh Government has statutory responsibility for operating and maintaining the M4 and trunk road network in Wales and leads on the Wales & Borders rail franchise.

EMERGENCY SERVICES

Overview

For the sector as a whole, the interconnectivity of the sector’s network and its geographic spread affords it a considerable degree of resilience to disruptive challenges, including flooding, by channelling key services through unaffected sites. In addition, cross sector agreements are in place to facilitate inter service mutual aid arrangements as and when necessary. The sector is also required to undertake business continuity planning as part of its duty under the Civil Contingencies Act 2004.

POLICE

Overview

There are well embedded arrangements in place for coordinating resilience across the police forces of England and Wales, ranging from self-assessment to inspection.

Sector Approach

The Association of Chief Police Officers (ACPO) has reviewed its published standard for contingency arrangements within the service, which describes ways and measures to integrate resilience to natural hazards into existing governance arrangements.

Assessment of vulnerability

As a category 1 responder under the Civil Contingencies Act 2004 the police service is required to undertake business continuity planning. The geographic spread of the service, together with its tried and tested mutual aid and mobilisation arrangements, result in the sub-sector being inherently resilient to disruption from natural hazards. A report by Her Majesty’s Inspectorate of Constabulary (HMIC) on civil contingency planning (2009) reported that business continuity planning was well integrated in forces but reminded them of the need to make sure key staff were aware of arrangements with adequate testing of those arrangements taking place.

Building resilience

The police service considers robust Business Continuity arrangements and Interoperability (seamless working arrangements) to be essential to achieving sector resilience and will continue to develop and scrutinise development in these two areas.

ACPO continues to offer direction on the importance of business continuity and the need to maintain sector resilience by chairing bi-annual meetings of business continuity managers from all forces, and through the continued promotion of the ACPO standard for civil contingencies across the service.

This standard represents a minimum threshold for what every force should be capable of delivering, or of arranging to be provided from elsewhere. It provides an agreed national assessment framework as well as enabling individual forces to make risk-based assessments of their own vulnerabilities. In the longer term this will deliver:

- An understanding of vulnerability across the police forces of England and Wales, using risk assessment and inspection on a periodic basis;

- Further improvements in resilience across the sector that will ensure delivery of critical policing services during an emergency;

- A benchmark for quantifying and certifying those improvements;

- A mechanism for reporting progress against the standard and for showing changes made based on the understanding of risks and vulnerability;

- A process for embedding the principles of sector resilience and business continuity throughout the police service.

The police sector has already begun to respond to the emerging issue of vulnerability associated with severe space weather and technical briefings on this hazard have been given by the Centre for the Protection of National Infrastructure to the police national business continuity group. These briefings will then be cascaded down to individual forces so that they are able to respond according to local need.

Within their recent report on civil contingencies planning, HMIC reported a clear expectation that forces should have business continuity plans in place, key staff such as managers and supervisors should be aware of these plans and they should be tested and validated systematically with any improvements implemented.

To enable improved information sharing across forces, the police service has also developed the Police Online Knowledge Area (POLKA); a facility that uses social media technology to enable sharing of information across a group of individuals who share a common, professional interest. It opens up channels of communication that extend beyond office boundaries with the added protection offered by a secure environment and is hosted by the National Policing Improvement Agency (NPIA).

A Business Continuity link has been created on POLKA enabling all police forces to share good practice.

Background

There are forty-three police forces in England and Wales. Each has its own Chief Constable who is responsible and accountable to a Police Authority for delivery of policing services (including business continuity) at the local level.

Her Majesty's Inspectorate of Constabulary (HMIC) is the body that independently monitors and assesses police forces and policing activity; reporting on performance with the aim of encouraging improvement. There are three main ACPO working groups that monitor and report on issues that have bearing on sector resilience.

- ACPO Emergency Procedures
- ACPO Business Continuity
- ACPO Interoperability

The Association of Chief Police Officers (ACPO) is the independent, professionally-led strategic body that leads and coordinates the direction and development of policing in England, Wales and Northern Ireland. It is also a voluntary association of Chief Officers who bring together their experience and expertise to support others through portfolio responsibilities.

As a category 1 responder under the Civil Contingencies Act 2004, the police service undertakes business continuity planning to ensure the resilience of its critical infrastructure to a defined standard: the ACPO standard[14] for civil contingencies which was last reviewed in February 2010. To aid compliance, ACPO chair a national group of police sector business continuity managers.

Chief Constables have their own policing plan which sets out the priorities for which they are responsible and accountable for delivering. Progress against a policing plan is reported to a Police Authority and they have a statutory duty to secure the maintenance of an efficient and effective police force. This includes making sure that the force is resilient, has a proper business continuity plan in place and ensuring that it is fully scrutinised by members of the Police Authority.

AMBULANCE

NHS Ambulance services range from orthodox "blue light" services to urgent (but non-emergency) care, clinical advice by telephone and patient transport. These are provided by eleven NHS ambulance trusts in England. In general, disruption to the ambulance service from natural hazards is more likely to arise as a result of the wider impacts of an event, e.g. road closures caused by flooding, rather than through direct impacts upon its fixed infrastructure.

The Ambulance Service is a devolved issue.

Further information on the approach to resilience planning in this sub-sector can be found in the Health Sector section of this document.

[14] Protective Services Minimum Standards http://www.acpo.police.uk/asp/policies/Data/Protective%20Services%20Minimum%20Standards%20Website.pdf

FIRE AND RESCUE

Overview

All fire and rescue control sites have fallback arrangements to divert calls to another fire and rescue service control site and set up secondary control sites following a disruptive event.

Sector Approach

As sponsor department for the fire and rescue services in England, the Department for Communities and Local Government (DCLG) has reviewed the quality of existing governance and generic contingency arrangements that underpin the delivery of critical services during periods of disruption.

Assessment of Existing Vulnerability

Each fire and rescue authority is required to:

- Have in place a plan to provide such level of emergency cover as it regards as appropriate during any period of emergency, liaising as necessary with other relevant organisations, but without reliance upon support of the Armed Forces;

- Ensure the availability of all necessary vehicles, equipment, training and support; and

- Have in place arrangements for heightening public awareness and vigilance in respect of safety issues during periods of emergency cover

In September 2010, the Audit Commission published a report, commissioned by DCLG on Business Continuity in the Fire and Rescue Service. The report looked at a range of business continuity events, including pandemic flu, flooding, extreme weather conditions, and industrial action, and concluded that all fire and rescue authorities have satisfactory business continuity plans in place.

However, the Report recognised some areas where the Fire and Rescue Services could improve their contingency planning, including:

- Involving local people more in deciding what an appropriate level of service means for them;
- Carry out further testing and exercising of plans to assure services that they have enough capacity and skills to provide enough cover;
- Collaborating further with partners and other fire and rescue services to build capacity and maximise resilience in a way that shows the best value for money for local people.

Fire and Rescue Services are particularly dependent on communications, for which they adopt a multilevel approach across logically and physically separate radio communications systems to ensure operational effectiveness:

- Radio communications between control rooms, fire appliances, officers’ cars and other support vehicles is provided by the Airwave ground based resilient network. Predominantly the existing 46 fire service control rooms connect to the Airwave service through radio interfaces
- Multi service interoperability is provided through the Airwave service
- At incidents, fire and rescue services use self-provided set-to-set analogue radio which requires no external infrastructure and is not reliant on any part of the Airwave service. This provides for voice communications and some service interoperability
- Part time firefighter mobilising is provided by local group paging systems (alerters) generally centred around individual fire stations
- Each fire and rescue service control room has an Imarsat terminal for use in the event of a widespread failure of other communications services
- As part of the new dimension provision, a number of enhanced communication vehicles will be deployed. These will provide limited uncontended bandwidth via VSAT (two way satellite link) between vehicles and the fixed ground fire service national coordination centre without the need for any ground infrastructure. Other satellite services are used by new dimension for specialist applications
- Commercial mobile phone voice and data services are also used to support non time critical communications requirements.

Building Resilience

To supplement existing assurance levels within the sector, DCLG recommended that fire and rescue services follow recognised business continuity management practices, such as those contained within BS25999 Part 1, when producing business continuity plans.

DCLG will continue to work closely with the Devolved Administrations, where the Fire and Rescue Service is devolved, to ensure that, in the event of a loss of a fire and rescue service critical national infrastructure (CNI) site, suitable and sufficient levels of resilience are maintained across the United Kingdom.

Background to the sector

Within England there are 46 fire and rescue authorities providing fire and rescue services in cities, towns and rural communities across the country.

The Fire, Resilience and Emergencies Directorate and the Office of the Chief Fire and Rescue Adviser within DCLG work with local fire and rescue authorities to help prevent deaths, injuries and damage to property. It also works in partnership with the fire and rescue services and other agencies to build the resilience and capability to deal with major emergencies, including terror attacks and natural disasters.

DCLG also publishes the National Framework for the Fire and Rescue Service,[15] which sets out the expectations of the Government for the fire and rescue service, and the support Government will provide in helping to meet these objectives.

The provision of services for fire-fighting, road traffic accidents, any other emergency function the Secretary of State may confer, by order, on a fire and rescue authority and promoting fire safety is the responsibility of the fire and rescue authority under the Fire and Rescue Service Act 2004. The Act also provides fire and rescue services with the power to respond to other eventualities it considers appropriate under the Act. This may include natural events such as flooding or manmade incidents such as terrorism.

[15] www.communities.gov.uk/documents/fire/pdf/nationalframework200811.pdf

HEALTH

Overview

The size of the National Health Service (NHS), coupled with the wide geographic distribution of individual assets and the ability to relocate key services to alternative sites in emergencies, provides an inherent degree of resilience in the sector. The NHS has robust procedures in place to respond to disruptive events but does have many critical dependencies with other infrastructure sectors including, energy, communications, water, food, and transport.

Sector Approach

As sponsor department for the health sector, the Department of Health has reviewed the quality of emergency preparedness across NHS funded organisations and outlined plans for the future.

Assessment of Existing Vulnerability

Following publication of the *White Paper, Equity and Excellence: Liberating the NHS* the health service is set to embark on a programme that will result in significant change to how the NHS delivers its services to the public. The health service has a good record of delivering widespread change while ensuring that services to the public are not disrupted. The Department of Health's Operating Framework for the NHS in England (2011 / 12) provides guidance for the health service on the restructuring programme and makes clear that emergency preparedness remains a high priority:

"All NHS organisations, other contracted healthcare providers, local authorities and other local organisations should maintain and test plans to deliver an effective response to threats and hazards. They should have robust and tested command and control systems, as well as meeting their local obligations under the Civil Contingencies Act 2004".[16]

The Department of Health has worked closely with the British Standards Institute and other interested parties to produce the Publicly Available Specification - PAS 2015; Intended for use by health service emergency planners, business continuity planners, estate managers and other involved in the resilience of organisations providing healthcare, the specification provides a resilience framework for all NHS funded organisations. In particular, PAS 2015:

- Helps to drive compliance with the relevant legislation, particularly the Civil Contingencies Act 2004;

- promotes a consistent approach to, and understanding of resilience;

[16] www.nhsemployers.org/managingthetransition/operating-framework/pages/operating-framework.aspx

- Defines the importance of resilience in the context of health;
- Highlights critical dependencies and the importance of building strong working relationships with suppliers;
- Promotes the principles of the British business continuity standard BS25999 throughout the service;
- Provides tangible and practical methods for applying and embedding resilience throughout NHS funded organisations.

In addition, the Department of Health has produced a Health Building Note, which provides guidance for health service providers on assessing, developing and implementing resilience – the ability of a building or engineering installation to withstand threats and hazards. It explains how to estimate the level of resilience required in a facility, how to develop an appropriate emergency plan and how to ensure resilience in the procurement process.[17]

The NHS has been able to integrate resilience into the day-to day management of its estates. All staff have a responsibility to report any defect or failure that occurs at work to the Department of Health, including failures in the critical services (electricity, water, steam, gas, communications etc).

Building Resilience

The Department of Health is developing a resilience framework for critical infrastructure in the sector, covering issues including consideration of resilience standards, and associated governance and funding issues.

The Department will also continue to implement PAS 2015: Framework for Health Services Resilience across the service and monitors progress through the National Capability Survey, which the sector is required to complete.

Background

The health sector in England incorporates a large number of organisations, providing a wide variety of different services. Types of patient care offered by the NHS include locally administered primary care (provided through 29,000 GPs in more than 8,200 independent practices), hospital-based acute care (provided through more than 200 hospitals of varying types), and inpatient or community-based mental health care. The significant majority of acute hospitals and the sector's support services operate under the auspices of the NHS, and thus lie within public ownership. As health is a largely devolved issue, the remit of the Department of Health only covers the NHS in England, but strong working

[17] www.dh.gov.uk/en/publicationsandstatistics/DH_4118956

relationships are maintained with the Devolved Administrations.

The majority of organisations within the health sector have responsibilities under the Civil Contingencies Act 2004 and are therefore required to maintain robust business continuity and emergency management plans. The Department of Health has responsibility for the strategic direction of emergency preparedness policy in the health sector in England.

FOOD

Overview

The UK has a highly effective and resilient food supply chain, providing wide consumer choice. The food retailers have robust and resilient business continuity plans to deal with any threat of disruption as demonstrated by the floods of 2007, the severe winter weather of January and December 2010.

Sector Approach

As sponsor department for the Food sector in England, the Department for the Environment, Food and Rural Affairs (DEFRA) has reviewed the resilience of the sector to pandemic flu, flooding, volcanic ash extreme cold plus snow events. In Wales, the Welsh Government has conducted a review of resilience within the food supply chain and in Scotland, the sector has prepared a separate Sector Resilience Assessment.

Assessment of Vulnerability

The commercial pressures that have promoted the drive for efficiencies have created a just-in-time culture in food distribution that requires an immediate response to an interruption to production or supply. Coupled with the number of supply chains, manufacturing and retail options and the high degree of substitutability of foodstuffs in the industry, the sector is extremely resilient to disruption. However, the sector is critically dependent on other infrastructure sectors, notably energy, transport, water and communications.

The Centre for Protection of the National Infrastructure (CPNI) completed a review of criticality of assets and products in the food sector in August 2009. This looked at nine sub-sectors - agriculture, fisheries, food ingredients production, food manufacture, packaging and other materials, storage and distribution, food retail, food service and waste disposal - and failed to identify any single critical asset that might affect the supply of food.

The food sector demonstrated its ability and flexibility to deal effectively with the 2007 floods in Gloucester and the South-West where the supermarkets remained open and able to provide food to the affected populations and, with the dairy and alcoholic drinks industry, the provision and distribution of water. During the severe weather of January and December 2010, the food retail & wholesale distribution sector continued to operate to near capacity.

Building Resilience

Owing to the large size of the food industry and the competition that exists within the various sectors, it is down to individual companies to review business continuity arrangements and plan for dealing with incidents such as flooding.

Background

The Food sector consists of sub-sectors of 522,000 food enterprises in the UK including Manufacturing, Storage & Distribution, Retailing and the Food Service.

Food is a devolved issue. In Scotland, the sector has prepared a separate Sector Resilience Assessment to complement the work undertaken in England and Wales.

Defra and the Welsh Government work with the food industry to promote an understanding in the relevant government departments of its dependencies. Defra set up and chairs the Food Chain Emergency Liaison Group, a forum at which other government departments, industry, and the relevant trade associations can share information and jointly consider developing government policy in this field. This meets three to four times a year and has considered issues that might affect the food sector, such as a flu pandemic and interruptions to fuel, gas or electricity.

FINANCE

Overview

HM Treasury, working with the Bank of England, the Financial Services Authority and industry, has successfully integrated a culture of continuous improvement in the resilience of the UK finance sector's critical infrastructure to natural hazards. This, combined with a natural competition between firms and correspondingly high levels of investment in business continuity, has meant that the sector has been able to secure a high standard of resilience to a range of natural hazards, although it remains highly dependent on the supply of its key utilities, particularly telecommunications and energy.

Sector Approach

The Financial Authorities, HM Treasury, the Bank of England and the Financial Services Authority (FSA) (referred to as the Authorities), share responsibility for ensuring the resilience of the financial sector.

For the 2010/11 Sector Resilience plan, HM Treasury has reviewed the resilience of the financial sector's critical infrastructure to coastal and fluvial flooding and highlighted critical dependencies with other national infrastructure sectors.

Assessment of Existing Vulnerability

The sector's critical infrastructure that is at risk of flooding have robust contingency plans in place and the capability to switch to an alternative site with the minimum of disruption to service.

This capability will be further enhanced by their continued participation in future sector-wide business continuity exercises led by the Authorities, as this raises awareness of relevant risks, tests resilience plans and trains staff.

A key dependency of the Finance Sector is telecommunications, as telecoms are required for all payment systems. Resilience to small scale disruptions is therefore built into these systems, however, the complete failure of the Public Switched Telephone Network or Internet Protocol networks would severely disrupt financial transactions for the period of the outage.

The sector is also dependent on the uninterrupted supply of electricity. To manage loss or shortages in the supply of electricity, all major institutions have backup capability in place.

Building resilience

The Authorities conduct a number of regular programmes of work to improve their and the sector's resilience to disruption, including:

- Sector-Wide Exercising: Since 2003, the Authorities have run a regular programme of Market-wide Exercises (MWEs), which aim to improve the sector's preparedness for dealing with major operational disruption;

- Resilience Benchmarking: The FSA has undertaken two Resilience Benchmarking exercises involving approximately 60 firms and financial infrastructure providers;

- Authorities' Exercising: The Authorities run an annual exercise to test their ability to respond to major operational disruption to the financial sector using their joint incident response framework;

- Industry Groups: The Authorities chair or are members of a number of industry groups. These groups provide an opportunity for the Authorities to engage with key firms and groups of firms on resilience, business continuity arrangements and arising threats and hazards, and provide an opportunity for sharing best practice;

- Financial Sector Continuity Website: The Authorities maintain a dedicated website for disseminating business continuity information to the financial sector. [18]

To enhance Government's understanding of the sector's resilience to all hazards, HM Treasury will develop, and incorporate in the 2011/12 Finance Sector Resilience Plan, a methodology for providing an assessment of the resilience of the sector to all hazards.

HM Treasury has also initiated work aimed at improving the Authorities' understanding of telecommunications resilience, including how to improve the relationship between financial institutions and their key service providers.

Further analysis of the impact of severe space weather on the financial sector will be undertaken following the results of a cross government risk assessment.

Background

As sponsor department for the financial sector HM Treasury is responsible for designating financial sector critical infrastructure and accounting for sector resilience to operational disruption. It fulfils both these roles in partnership with the Bank of England and the FSA.

The Bank of England and the FSA are responsible for regulatory oversight of the UK financial sector, the Bank having oversight of payment systems and the FSA regulating firms and recognised bodies.

Part 5 of the Banking Act 2009 established a new statutory framework

[18] www.fsc.gov.uk

for the Bank of England’s oversight of financial market infrastructure. This conferred responsibility on the Bank of England to formally oversee recognised systems whose disruption might (a) threaten the stability of, or confidence in, the UK financial system; or (b) have severe consequences for business or other interests throughout the UK. The Act includes powers for the Bank to impose penalties on such systems where compliance failures are committed.

The FSA’s powers and responsibilities are set out in the Financial Services and Market Act 2000. The subsequent regulatory policy actively promotes the resilience of authorised firms, exchanges and clearing houses.

The Authorities’ work on financial sector resilience is directed by the Standing Committee on Financial Stability. The Standing Committee comprises senior representatives of the Treasury, Bank of England and the FSA. The Committee is chaired by the Treasury.

A sub-group of Standing Committee coordinates the Authorities’ joint work on financial sector resilience to operational disruption and maintains and tests tripartite arrangements for effective crisis management in an operational disruption. This group is also chaired by the Treasury.

Regulatory oversight of the UK’s financial sector is currently under review along the lines of proposals set out in the consultation document, *A new approach to financial regulation: judgement, focus and stability.* [19]

[19] www.hm-treasury.gov.uk/consult_financial_regulation.htm

GOVERNMENT

Overview

The diverse nature of the Government sector makes the sector inherently resilient, however, it depends heavily on other sectors such as energy and communications. A number of cross departmental initiatives on risk assessment and business continuity make it well placed to deliver continual improvements in infrastructure resilience to disruption from natural hazards.

Sector Approach

As sponsor Department for the Government Sector, the Cabinet Office, has reviewed the quality of existing governance and generic contingency arrangements that underpin the delivery of resilience in Government services and the estate.

Assessment of Existing Vulnerability

The Government sector comprises a large number of assets carrying out a wide variety of operations. They include government departments themselves, but also national crisis response facilities, information networks, data centres, laboratories and many others supporting the functions of government.

Essential services that the sector provides include:

- The delivery of frontline services to the public (e.g. welfare payments);
- The management of the State's finances (e.g receiving and managing tax income);
- The provision of scientific advice (e.g animal and human health laboratories);
- The development, implementation and review of legislation and Central Government policy;
- National response to emergencies.

At the Sector-wide level, the lack of interconnections across the sector's critical infrastructure reduces the risk of cascade failure, where the loss of one asset could lead to the loss of further vital assets (i.e. the loss of a welfare payment site will not affect the management of the UK's armed forces). The appraisal of specific risks to the sector can therefore be relatively straightforward e.g. the 2010 Government Sector Resilience Plan assessed the vulnerability of the most critical sites in the sector to flooding.

However, differences between departments in the understanding and assessment of risks to infrastructure makes it far more difficult to appraise the resilience of the sector as a whole i.e. on an 'all-risks', cross-departmental basis. In addition, the sector is reliant on essential services such as energy and telecoms and therefore these dependencies also need to be understood.

The Cabinet Office is therefore continuing to work with other departments to bring together programmes on risk assessment, protective security, business continuity and internal audit in order to unify the approach to building infrastructure resilience.

Building Resilience

Lead Ministers are accountable to Parliament for all the policies, decisions and actions of their Departments; the management of their organisations; the use of public money; and the stewardship of its assets.

Departments discharge their functions through Corporate Governance systems. Corporate Governance is the way in which Departments are directed and controlled.[20]

A key part of these arrangements is the Statement on Internal Control. Lead Ministers sign this statement, which sets out their Department's processes for reviewing governance, risk management and control arrangements, which includes the safeguarding of the organisation's assets.

Departments are supported in this role by Her Majesty's Treasury Corporate Governance teams providing advice and best practice examples on effective corporate governance, risk management and internal audit.

Following production of the 2010 Government Sector Resilience Plan and subsequent discussions with officials, the Cabinet Office considers that, owing to the dynamic and changing risk from natural hazards and the complexity of the Government sector, continuous improvement in the resilience of critical infrastructure is best achieved by Departments through:

- Regular Board level consideration of matters relating to the resilience of critical infrastructure alongside other organisational priorities;
- Ensuring the full integration of the National Risk Assessment (NRA) and the Security Policy Framework (SPF) into business risk management strategies;
- Board commitment to the design, implementation and review of an organisational resilience strategy;
- Closer operational working relationships between departmental security officers, business continuity planners; risk improvement managers, asset managers and, externally, supply chain partners and emergency responders on infrastructure resilience.

To support Departments to improve the resilience of their infrastructure to natural hazards, the Cabinet Office has initiated a programme of work under the existing Critical

[20] Governance is defined as "the combination of processes and structures implemented by the Board (senior management) to inform, direct, manage and monitor the activities of the organisation toward the achievement of its objectives." HM Treasury. Internal Audit Standards. April 2009. Page 35.

Infrastructure Resilience Programme (CIRP). Its aims are to challenge and support departmental boards to safeguard their organisation's assets to the risks identified in the National Risk Assessment 2010 and Security Policy Framework.

Embedding organisational resilience into governance mechanisms will ensure that the vulnerability of critical infrastructure to disruption from natural hazards is considered by departmental boards alongside other organisational priorities. Thereby, informing longer term strategic investment and procurement decisions, risk management and discussions with supply chain partners. It will enable Departments to improve their understanding of the resilience of their infrastructure, measure the success of the strategy at regular intervals, and make necessary amendments to secure delivery or to match changing organisational priorities / circumstances.

A requirement for Government Departments to undertake business continuity management is set out in the Security Policy Framework.[21] Departments are supported in their business continuity planning through a Cabinet-Office led cross-departmental forum.

To ensure a level of consistency and an objective review of the quality of contingency planning by departments, the Government uses a system of Independent Internal Review. The Independent Internal Review is a process jointly owned between the Cabinet Office and the staff of the Emergency Planning College. This process combines the expertise of central government and private sector security-cleared staff with in-depth knowledge of the public sector.

To support departments in undertaking their risk assessments, the National Risk Assessment (NRA) is shared across the sector. The NRA is produced annually by the Cabinet Office and provides a collectively agreed assessment of the relative significance of potential malicious and non-malicious disruptive events that would cause significant harm and disruption to the UK.

The Critical Infrastructure Resilience Programme will continue to work closely with these programmes to devise and implement a programme of work across departments that further enhance the security and resilience of the Government estate to all risks.

Background

The Government Sector is wholly owned and managed by the UK Government, although the management of some of the assets is outsourced to private contractors (e.g. the management of information technology data centres).

[21] HMG Security Policy Framework, version 4, Cabinet Office May 2010. www.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf