Cabinet Office

A Summary of the

2012 Sector Resilience Plans

May 2012

Produced by:

Cabinet Office
35 Great Smith Street
LONDON
SW1P 3BQ

www.cabinetoffice.gov.uk

Contact:

Civil Contingencies Secretariat

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

Publication date: May 2012

Contents

INTRODUCTION

1. Sector Resilience Plans set out the resilience of each national infrastructure sector to the relevant risks identified in the National Risk Assessment.[1] The Plans are placed before Ministers to alert them to any perceived vulnerabilities, with a programme of measures to improve resilience where necessary.
2. The national infrastructure is categorised into nine sectors: Communications, Emergency Services, Energy, Finance, Food, Government, Health, Transport and Water (see Table 1). 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]
3. Working with infrastructure owners and regulators, the Government departments responsible for the nine national infrastructure sectors are required to produce Sector Resilience Plans on an annual basis. For 2012, Plans have also been produced for the Nuclear and Hazardous Sites sectors. The process is coordinated by the Civil Contingencies Secretariat (based in the Cabinet Office).
4. This is the third round of Sector Resilience Plans: the 2010 planning round assessed the risk to UK's most important infrastructure from inland and coastal flooding; the 2011 round extended the scope to all natural hazards; and the 2012 planning round has extended the scope further to allow departments to review the resilience of their most important infrastructure to all risks (threats and hazards).
5. Owing to their sensitive nature, individual plans are classified. This document presents an unclassified summary of the 2012 Plans.

[1] The National Risk Assessment is the main document Government uses to assess the major threats (malicious terrorist attacks) and hazards (non malicious risks such as human and animals diseases, industrial accidents and industrial action, natural hazards such as flooding and drought) the UK could face in the next five years. A public summary is available at: www.cabinetoffice.gov.uk/resource-library/national-risk-register

[2] 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).

TABLE 1. INFRASTRUCTURE SECTORS, ASSOCIATED SUB-SECTORS AND LEAD GOVERNMENT DEPARTMENTS

Sector	Sub –Sector(s)	Sector Resilience Lead [3]
Communications	Broadcast	Department for Culture, Media and Sport
	Postal	Department for Business, Innovation and Skills
	Telecoms	Department for Business, Innovation and Skills
Emergency Services	Ambulance	Department of Health
	Coastguard	Department for Transport
	Fire & Rescue	Department for Communities and Local Government
	Police	Home Office
Energy	Electricity	Department of Energy and Climate Change
	Gas	Department of Energy and Climate Change
	Oil	Department of Energy and Climate Change
Finance		HM Treasury
Food		Department for Environment, Food and Rural Affairs
Government		Cabinet Office
Hazardous Sites		Department for Business, Innovation and Skills
Health		Department of Health
Nuclear		Department of Energy and Climate Change
Transport	Aviation	Department for Transport
	Ports	Department for Transport
	Rail	Department for Transport
	Road	Department for Transport
Water		Department for Environment, Food and Rural Affairs

[3]Where responsibility for the resilience of the sector sits with a Devolved Administration, relevant Government Departments and the Devolved Administrations worked together to ensure the 2012 Sector Resilience Plans covered the entirety of the UK.

GOVERNMENT'S APPROACH TO BUILDING INFRASTRUCTURE RESILIENCE [4]

Infrastructure resilience is the ability of assets and networks to anticipate, absorb, adapt to and recover from disruption. Resilience is secured through a combination of the principal components shown in Figure 1.

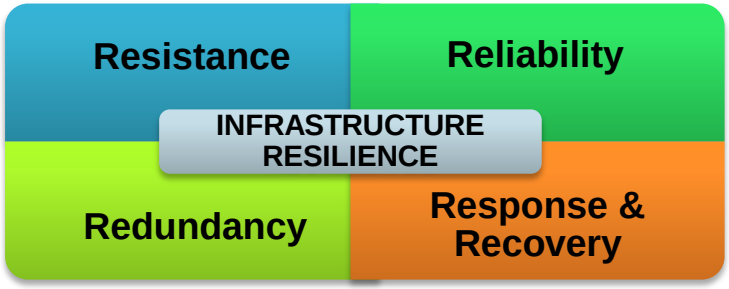

Figure1: The components of Infrastructure Resilience

- **Resistance.** Concerns direct physical protection, e.g. the erection of flood defences;
- **Reliability.** The capability of infrastructure to maintain operations under a range of conditions, e.g. electrical cabling is able to operate in extremes of heat and cold;
- **Redundancy.** The adaptability of an asset or network, e.g. the installation of back–up data centres; and
- **Response and Recovery.** An organisation's ability to respond to and recover from disruption.

Tripartite Approach

The appropriateness and cost-effectiveness of each component varies across the sectors owing to, for example, the different types of infrastructure, technical opportunities and business models. Infrastructure owners should work with Government and regulators to select the blend of these components which will produce the most cost effective and proportionate strategy.

Role of Sector Resilience Plans

The sector resilience planning process provides the opportunity for Government, regulators and infrastructure owners to work together to produce a mix of resilience components that are:

- proportionate to the risks identified in National Risk Assessment products;
- enabled by improved sharing of information; and
- in keeping with legal and regulatory frameworks, industry standards, licence agreements and business models.

[4] The Government's advice on improving the resilience of infrastructure is set out in the document: *Keeping the Country Running: Natural hazards and infrastructure.* www.cabinetoffice/infrastructure-resilience

COMMUNICATIONS

Summary. The Communications sector is made up of the Telecoms, Postal and Broadcast sub-sectors. Each sub-sector has invested proportionately in its resilience to risks including those identified in the National Risk Assessment. The sector is vulnerable to prolonged and widespread disruption of other essential services, particularly energy, and damage to or destruction of its key infrastructure.

Assessment of Existing Resilience

1. Within each sub-sector, resilience building is driven by a combination of competition, new technologies and the need to meet legislative requirements, licences or standards.
2. The sector is vulnerable to prolonged disruption to electricity supplies, transport networks, for postal services in particular, and damage or destruction to its internal assets and networks.
3. To build resilience to disruption from failures within internal networks or other essential services, the sector has installed, or is installing, contingencies such as: alternative power supplies; back-up control and data centres; and the capability to perform critical functions from multiple sites.
4. Where necessary, most organisations have followed expert advice to protect key sites and networks from physical and electronic security threats and natural hazards in line with current risk assessments by, for example, completing personnel security vetting and erecting flood defences.
5. Prolonged, widespread disruption to energy supplies, and transport networks could disrupt the delivery of services across the sector.

Building resilience

6. Work continues with partners and expert agencies to:

- **Sector- wide**. Maintain compliance with domestic and international legislation, licence agreements and consider the impacts of other potential risks to the sector such as severe space weather;
- **Telecoms and Broadcast.** Ensure that resilience plans incorporate the risk of cyber attack; and
- **Postal.** Complete resilience-focussed site improvement programme.

EMERGENCY SERVICES

Summary. The Emergency Services sector is made up of the Police, Ambulance, Fire and Rescue, and Maritime and Coastguard Agency. Compliance with civil protection legislation, the interconnected nature of its networks, well tested mutual aid agreements and the geographic spread of services across the UK affords the emergency services sector a considerable degree of resilience to disruption from major risks.

Assessment of Existing Resilience

1. Emergency Services are subject to the full set of civil protection duties under the Civil Contingencies Act (2004), including the requirement to assess the risk of emergencies to inform preparations and put in place emergency and business continuity plans.
2. The major risks to the sector are loss of communications and loss of power. Of these, the sector is particularly dependent on communications. However, operational effectiveness in times of disruption is managed by the use of a range of satellite and radio communications options.
3. To support emergency response during periods of disruption from major and other risks, each service has:

- well tested fall back arrangements, including back up operation centres and back up power supplies;
- the ability to divert emergency calls between call centres;
- complied with the HMG Security Policy Framework;[5]
- inter-service mutual aid agreements underpinned by:
    - compatible communications and control rooms;
    - multi-agency plans, training and exercising; and
    - shared understanding of operational procedures.

Building Resilience

4. To enhance mutual aid activities, the emergency services will continue to work together to improve connectivity of services. Work to consider the criticality and vulnerability of key sites in an ever changing risk environment will also be a priority.

[5] The HMG Security Policy Framework sets the protective security mandatory standards and best practice guidelines and compliance is monitored through an annual reporting process.

ENERGY

Summary. The energy sector is made up of the upstream oil and gas, electricity generation and electricity networks. Although infrastructure types and business environments differ, each sub-sector has invested proportionately to build resilience to major risks, but the size of networks mean improvements can take years to complete.

Assessment of Existing Resilience

1. Major risks to the energy sector are flooding, wind and loss of key staff. To build resilience to these and other risks, energy companies are required or advised to:

- **adopt an all risks approach**. Under the Utilities Act 2002, Ofgem introduced performance levels for the gas and electricity industry including supply restoration timescales;
- **address specific vulnerabilities.** Companies have improved clearance between overhead lines and vegetation to minimise disruption from windborne debris; and
- **put in place contingency arrangements.** Energy companies have worked extensively to put in place contingency plans to manage staffing in the event of pandemic influenza.

2. Owing to the size and complexity of energy networks, completion of programmes can take a number of years, meaning that while vulnerabilities are being addressed, there is an ongoing, but reducing, risk of disruption.

Building Resilience

3. Priorities include:

- **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;
- **Electricity Networks.** Assessment of the risk posed by severe space weather; and completion of the electricity networks vegetation management programme.

FINANCE

Summary. The financial sector has been able to secure a sufficiently high standard of resilience to a range of major risks, reflecting a mature approach to resilience and ongoing investment by firms. The sector is vulnerable to significant disruption to other essential services, particularly energy and telecoms.

Assessment of Existing Resilience

1. The major risks to the sector are disruption to energy and communications networks, and damage or destruction to key financial assets and networks.
2. To lessen the impact of electricity and telecoms disruption firms have, for example:
   - invested in uninterruptible power supplies;
   - built back up data centres; and
   - held industry-wide exercises to test the response to and recovery from major utility failure.
3. To protect the integrity of assets and networks, the sector has worked with expert agencies to:
   - address vulnerabilities in the physical integrity of key assets and networks to terrorist threat, severe space weather and flooding, for example;
   - improve the security of information networks to cyber attack; and
   - complete personnel security checks.
4. Irrespective of the cause, the Financial Authorities require firms to maintain services in the event of an unforeseen interruption, as far as is reasonable. [6]
5. The sector has built resilience to short term disruption to energy and communications networks. Lengthy or widespread disruption of these networks, possibly as a result of complex risks such as severe space weather or cyber attack, could challenge the delivery of financial services.

Building Resilience

6. The sector will progress existing work to evaluate the impact of severe space weather and cyber attack on financial assets and networks directly, and indirectly from disruption to energy and communications networks.

[6] The Financial Authorities include, HM Treasury, Bank of England and the Financial Services Authority

FOOD

Summary. The UK food sector has a highly effective and resilient food supply chain, owing to the geographic spread, number of firms and competitive nature of the industry. Its resilience has been demonstrated by several recent disruptive challenges, although there is a widespread dependency on other essential services.

Assessment of Existing Resilience.

1. The commercial pressures of the food sector have created a just-in-time culture 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 resilient to disruption.
2. This resilience has been demonstrated in recent nation-wide events such as the 2007 floods (where the supermarkets remained open and able to provide food to the affected populations and the dairy and alcoholic drinks industry able to provide and distribute water), the 2009 H1N1 Pandemic and the 2010 Icelandic volcanic ash clouds.
3. More recently, the food retail & wholesale distribution sector continued to operate to near capacity despite the severe winter weather experienced during January and December 2010. However, the sector recognises that it is critically dependent on the energy, transport (particularly ports), water and communications sectors.

Building Resilience.

4. In the coming year, the sector will research its vulnerability to transport disruption. In particular, research into the resilience of food supply to port disruption will improve understanding of potential food disruption in the event of problems at ports such as bad weather, port closure or staffing issues. Further research will look at the resilience of rural communities' food supply chain.

GOVERNMENT

Summary. A range of essential services are delivered by the Government sector and these services are supported by a variety of infrastructure types. Effective risk management and contingency arrangements enhance the capability of Departments to respond to disruption their infrastructure but work is currently underway to improve the capability of Departments' to understand the risks to their key assets.

Assessment of Existing Resilience

1. The Government sector delivers a variety of essential functions, including the delivery of public facing services (e.g. welfare payments), management of State finances, provision of scientific advice and the national response to emergencies.
2. All of these are reliant on the provision of power supplies, telecommunications and key staff, the loss of which are the major risks to the sector.
3. To prevent disruption from and ensure an effective response to these and other risks Departments must:

- have well tested business continuity and emergency response plans;[7]
- comply with the HMG Security Policy Framework;[8] and
- report to Parliament on the effectiveness of risk management procedures.

4. To date Departments have focused on improving their internal preparations to an emergency. The resilience of the sector would benefit from a more collaborative approach that places emphasis on the protection of key sites to major risks.

Building Resilience

5. To complement sector-wide efforts to deliver an effective emergency response, Departments will work together to improve the resilience of the sector to major risks, particularly the capability of key infrastructure to withstand and absorb disruption.

[7] Departments' business continuity plans must be aligned to the business continuity British Standard, BS 25999.

[8] The HMG Security Policy Framework sets the protective security mandatory standards and best practice guidelines and compliance is monitored through an annual reporting process to Cabinet Office.

HAZARDOUS SITES

Summary. The need to comply with stringent safety legislation and conventions promote the resilience of the sector's infrastructure to the most relevant risks. To complement efforts to prevent casualties from chemical release and prevent the misuse of substances, work has begun to review the resilience of sites whose activities support the delivery of essential services.

Assessment of Existing Resilience

1. The requirement for asset owners in the sector to comply with safety legislation or conventions promotes resilience. For example:

- sites governed by the Control of Major Accident Hazard (COMAH) regulations must put in place proportionate measures necessary to prevent and respond to major accidents;[9] and
- sites producing certain quantities of particular chemicals are, under the Chemical Weapons Convention (CWC), subject to data monitoring, licensing and inspection.

2. At the local level, to support site protection and incident response, police forces work with infrastructure owners to maintain emergency plans and a list of hazardous substances on-site.
3. As the challenge set by legislative requirements to firms depends on the type and / or quantity of substance produced on site, standards of resilience can vary across the sector.
4. Previously, sector resilience building has focussed on preventing casualties following chemical release and preventing the misuse of substances. However, the loss of some sites could disrupt the flow of chemicals to essential services effectively disrupting the provision of these services to the public.

Building Resilience

5. The sector's priority will be to further existing work to enhance the security and resilience of sites whose loss carries the greatest risk to people and to consider the impacts on delivery of essential services.

[9] COMAH safety reports address protection measures against a variety of scenarios including, where appropriate, flooding, earthquakes, high winds and extreme weather.

HEALTH

Summary. The NHS is a large, complex, interconnected set of healthcare services. The need to comply with civil protection duties, and the adaptability of services and the service-wide desire to sustain the provision of healthcare ensures the NHS is able to manage most disruptive events. However, the NHS remains exposed to the risk of disruption to other essential services, particularly when demand for healthcare has also increased.

Assessment of Existing Resilience

1. The Civil Contingencies Act (CCA) and the NHS Operating Framework Emergency require the NHS to respond safely and effectively to major risks.[10]
2. As healthcare services and supplies are replicated throughout the UK and well-tested mutual aid agreements between services are in place, the NHS is inherently resilient to most major risks.
3. NHS organisations have invested in technologies and staff training to ensure an effective response to emergencies.
4. In addition, *PAS 2015: Framework for Health Services Resilience* provides all NHS organisations with a method for applying and embedding resilience.
5. However, the NHS remains dependent on the provision of utilities to sustain services over the longer term.
6. NHS services regularly manage short term disruption and high demand by invoking mutual aid agreements or curtailing non-critical services. As the NHS operates at near capacity, lengthy or widespread disruption of utilities could challenge the effective delivery of healthcare services, particularly if there is an increased demand for healthcare at the same time.

Building Resilience

7. To ensure a unified and cohesive approach to resilience building within and between all healthcare organisations (and suppliers), work to implement the principles underpinning PAS 2015 throughout the NHS will remain the focus.

[10] www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_131360

NUCLEAR

Summary. In addition to very high build standards, effective governance and a stringent regulatory regime help strengthen the nuclear sector's resilience to major risks.

Assessment of Existing Resilience

1. Working with the Department of Energy and Climate Change, the Office for Nuclear Regulation and the Civil Nuclear Constabulary, the sector has adopted an all risks approach to the safety and security of sites.
2. Infrastructure owners are required to comply with national standards regulating the safety and security of nuclear licensed sites. For example:

- **Security threats.** Regulators complete no-notice site inspections. Sites must carry out personnel security vetting and regular counter terrorism exercises.
- **Hazards.** Where necessary, sites must erect flood defences to resist a 1 in 10,000 year flood; and
- **Accidents.** Sites must install numerous safety barriers to prevent an accidental release of radioactive material.

Building Resilience

3. The Department of Energy and Climate Change has worked with partners in government, the regulator and industry to create a National Framework which:

- Establishes a national strategy for UK nuclear site emergency planning and response;
- Coordinates all partners involved in this work across the UK;
- Ensures high quality, well-tested emergency response and recovery plans for existing and new build sites; and
- Ensures effective communications with local, national and international audiences.

4. On 11 March 2011, Japan suffered its worst recorded earthquake. The resulting tsunami severely damaged Fukushima Dai-ichi nuclear power site triggering a national and international nuclear emergency.
5. Findings from Her Majesty's Chief Inspector of Nuclear Installations report, examining lessons from the Fukushima accident to enhance the safety of the UK nuclear industry, will support the National Framework.

TRANSPORT

Summary. The transport sector comprises the road, aviation, rail and maritime sub-sectors. Multi-agency emergency planning, investment in technological solutions and contingency supplies, plus the interconnected nature of its networks, all lend resilience to the sector. However, the scale and exposed nature of the network leaves it vulnerable to some significant risks.

Assessment of Existing Resilience

1. The major risks the transport network faces are severe weather, flooding, power outages, reduced fuel supplies and volcanic ash. To maintain essential services, transport operators have:

- **stockpiled emergency supplies.** Local Authorities and the Highways Agency have increased salt supplies to minimise disruption to the road network from snow and ice. The rail sector has placed standby generators at key sections to lessen impacts from power outages.
- **adopted a multi agency approach to planning.** To build an effective response and recovery to severe coastal flooding, Port Authorities, Local Authorities and Local Resilience Forums have worked together to raise awareness and develop guidance.
- **sought expert advice.** Network Rail is advised of flood warnings by the Environment Agency and has access to a dedicated weather forecasting website tailored to the rail industry.
- **invested in technical solutions.** Following the disruption caused by Volcanic Ash, the UK aviation industry has supported the provision of new radar cover in Iceland to enable more accurate data on eruptions, and a specifically designed civil contingency aircraft. Discussions on acquiring more scientific aids are at an advanced stage.

Building Resilience

2. Priorities include:

- placing increased emphasis on better co-operation between different transport sectors at crucial parts of the supply chain;
- working more closely with Local Resilience Forums to develop and test contingency arrangements; and
- considering the potential impact of new risks including severe space weather and cyber attack on the sector.

WATER

Summary. An all risks regulatory framework, mutual aid agreements and high levels of investment have strengthened the resilience of the water industry to major risks.

Assessment of existing resilience

1. The current major risks to the water sector are drought and the loss of some other essential services.
2. Irrespective of the risk, water companies are statutorily required to provide alternative water supplies should piped supplies fail.[11]
3. Water companies must also maintain specific plans to minimise the impact of drought. Drought is, at present, a significant challenge for the water sector and, where necessary, drought plans have been invoked.
4. Disruption to electricity supplies could result in the loss of mains water and affect the movement and treatment of sewerage. A loss of telecoms would impact the sector's remote flow management and monitoring system.[12]
5. Water companies have short term contingency plans in place for power, including back up generators. They also continue to develop multiple monitoring systems to reduce impacts of telecoms failure.
6. These resilience efforts are bolstered by an industry-wide mutual aid agreement to enable sharing of emergency equipment.

Building Resilience

7. In the previous price period, Ofwat made £400m available to companies' to improve the resilience of assets and systems to flooding and other hazards. Companies have been instructed to once again consider the resilience of assets to major risks in their business plans for the period 2010-2015. Immediate priorities will be to respond to and recover from the current drought.

[11] Security and Emergency Measures Direction 1998, www.cabinetoffice.gov.uk/media/132943/semd98.pdf

[12] Supervisory Control And Data Acquisition (SCADA) remotely manages the flow of sewage and treated water. It also monitors and records water quality data.