Cabinet Office

A Summary of the

2013 Sector Resilience Plans

November 2013

Produced by:

Cabinet Office
35 Great Smith Street
LONDON
SW1P 3BQ

www.gov.uk/government/organisations/cabinet-office

Contact:

Civil Contingencies Secretariat

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

Publication date: Nov 2013

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 2013, 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 fourth round of Sector Resilience Plans and, as with the 2012 plans, they 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 2013 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.gov.uk/government/publications/national-risk-register-for-civil-emergencies-2012-update

[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

[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.

	Rail	Department for Transport
	Road	Department for Transport
Water		Department for Environment, Food and Rural Affairs

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.

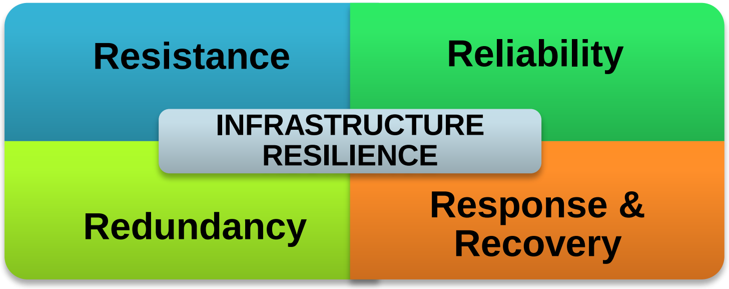

Figure1: The components of infrastructure resilience

- **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.gov.uk/government/uploads/system/uploads/attachment_data/file/78901/natural-hazards-infrastructure.pdf

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. To build resilience, 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.
3. 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
4. Prolonged, widespread disruption to energy supplies and transport networks could disrupt the delivery of services.

Building Resilience

1. Work continues with partners and expert agencies as follows:

Sector-wide

- To maintain compliance with legislation and consider the impacts of other potential risks to the sector.
- To ensure that robust contingency plans are in place to manage emergencies and restore service to customers.
- To strengthen relationships with Government, other agencies and industry through joint committees and working groups such as the Electronic Communications Resilience and Response Group (EC-RRG) for telecoms.

Telecoms and Broadcast

- To ensure that resilience plans incorporate the risk of cyber attack.

Postal

- To maintain 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. A strategic review of the scale of assets in the emergency services sector by CPNI, was initiated in 2013.

[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, downstream 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 infrastructure and networks mean improvements can take years to complete.

Assessment of Existing Resilience

1. Major risks to the energy sector are flooding, including coastal flooding, storms and gales, 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.
   - **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 on-going, 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; cyber-attack and completion of the electricity networks vegetation management programme.
   - **Downstream oil:** working on maintaining capability to make fuel deliveries in the event of a serious disruption.

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 and there is inevitably a limit to how far vulnerability to the most severe events can be reduced.

Assessment of Existing Resilience

1. The major risks to the sector are disruption to energy and communications networks, and damage to or destruction of 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 disruption to telecoms networks.

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
- improve the security of information networks to cyber attack, and
- complete personnel security checks.

4. 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

5. 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 other essential services, in particular communications networks. The sector will also consider lessons learnt from real life severe events.

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. Although this sector has a number of dependencies on other essential services such as fuel, the sector's resilience has been demonstrated by disruptive challenges in recent years.

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. However due to the number of supply chains, manufacturing and retail options available, coupled with the high degree of substitutability of foodstuffs in the industry, the sector is resilient to disruption.

2. This resilience has been demonstrated in nation-wide events such as the 2007 floods, the 2009 H1N1 Pandemic the 2010 Icelandic volcanic ash clouds and the 2012 potential industrial action by fuel tanker drivers.

3. Also, the food retail & wholesale distribution sector continued to operate to near capacity despite the severe winter weather experienced during January and December 2010 and January 2011. However, the sector recognises that it is critically dependent on the energy, transport (particularly ports), water and communications sectors and has strong contingency plans.

Building Resilience

4. In the coming year, the sector will build on recent research looking at the resilience of the food supply chain to port disruption and "pinch points" created by potential fuel disruption. Further research projects will provide an evidence base to strengthen the food industry's ability to respond to and recover from a major coastal flooding event, and build resilience in the supply chain to extreme weather events.

GOVERNMENT

SUMMARY: It is vital that Government can continue to perform its most essential services even if the face of disruptive challenges. To ensure this is possible, departments and a number of Government-wide programmes are working to ensure strong protective measures are in place to, where possible, prevent disruption and continually strengthen its ability to respond and recover from any disruption.

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 national response to emergencies.
2. Risk management is embedded within the Government sector and all Government departments and agencies are required to:
   - manage security and information risks to the standard set out in HMG's Security Policy Framework[6]
   - have tested business continuity and emergency response plans[7], and
   - report to Parliament on the effectiveness of risk management procedures.
3. Nevertheless, like other sectors, the Government relies on its buildings and on the power supply, its workforce and the integrity of its systems to perform its functions. Consequently, the loss of compromise of any of these could present significant challenges.
4. The Government sector's most critical assets are assessed to be adequately protected against the wide variety of risks facing Government and have business continuity plans that are generally of a high standard.

Building Resilience

5. Departments and a number of Government-wide programmes are working to ensure strong protective measures are in place to, where possible, prevent disruption and strengthen its ability to respond and recover from disruption. For example, as part of the National Cyber Security Programme, the Government continues to further develop its protection measures against cyber attacks.

[6] HMG's Security Policy Framework sets the protective security mandatory standards and best practice guidelines. Compliance is monitored through an annual reporting process to the Cabinet Office.

[7] Departments' business continuity plans must be aligned to the business continuity British Standard: BS25999.

HAZARDOUS SITES

SUMMARY: The need to comply with stringent safety legislation and internationally agreed 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 identify and review the resilience of those sites whose activities support the delivery of essential services.

Assessment of Existing Resilience

1. Resilience in the chemical sector is not mandated by regulation but the requirement for asset owners in the sector to comply with safety legislation or Conventions promotes a strong safety and working ethos. 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[8], and

   - sites producing certain quantities of particular chemicals are, under the Chemical Weapons Convention (CWC), subject to data monitoring, licensing and [international] inspection and the higher risk sites have been given security advice by CPNI and NaCTSO.

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. Leading sector trade associations require their members to adopt additional measures, going beyond just statutory, to enhance resilience efforts.

4. 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 legitimately vary across the sector.

5. Previously, sector resilience building has focussed on preventing or minimising casualties following chemical release and preventing the misuse of substances. However, the impact of other risks on some sites could disrupt the flow of chemicals to essential services thereby disrupting the provision of these services to the public.

Building Resilience

6. Work continues with stakeholders – site owners, sector organisations and across Government - to encourage and promote resilience issues. Relevant sites will be encouraged to consider their resilience to major risks and to develop mitigating measures so that the impacts to the public and to essential services will be minimised

[8] 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 organisation delivering its services through a large number of different healthcare settings within the new health and care system, which became fully operational from 1 April 2013.

It is important that the health sector is able to operate in a range of circumstances and continue to provide services to the public. Much work has been done on improving general resilience and business continuity planning, which is regularly reviewed and updated. The NHS is well versed in dealing with a range of disruptive events that stretch the resources of the health care system and is able to respond to a wide range of incidents on a daily basis.

In January 2013 NHS England published its Core Standards for Emergency Preparedness, Resilience and Response (EPRR), which is used to develop specific plans that are tailored to local risks.

Assessment of Current Resilience

1. The NHS must respond safely and effectively to major risks in line with the Civil Contingencies Act 2004 (CCA) and centrally provided EPRR standards and guidance.

2. Well tested mutual aid agreements between services, including ambulance, are in place and investment in equipment and technologies, along with staff training ensure an effective response to emergencies.

3. Local business continuity plans ensure that critical services can continue in the event of loss of utilities and agreements for priority re-connection are in place.

4. NHS services are regularly subjected to short term disruption or increase in demand which they manage by curtailing non-critical services and invoking mutual aid agreements. However, an incident that reduces staff availability as well as increasing demand on services would be very challenging for the NHS.

Building Resilience

5. Ensure a unified approach using Core Standards to suit local circumstances.

6. Constantly review and update plans, including business continuity, learning lessons from incidents as they occur.

7. Carry out a series of targeted site visits to review security of critical infrastructure.

CIVIL NUCLEAR

SUMMARY: High standards and well-established and tested emergency plans for each site, with an independent regulatory regime, provide resilience in the nuclear sector.

Assessment of Existing Resilience

1. Working with the Department of Energy and Climate Change (DECC), the Office for Nuclear Regulation and the Civil Nuclear Constabulary, the sector has made a comprehensive assessment of the risks to the safety and security of sites.
2. Licensed nuclear sites must comply with robust safety and security regulations and stringent licensing requirements with no-notice site inspections. For example:
   - **Security**. Site security plans must be approved by the regulator and measures include 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.
   - **Accidents.** Sites must have in place a series of safety measures to prevent accidents, alongside high quality, well-tested emergency response and recovery plans.

Building Resilience

3. Government, the regulator and industry have created a robust National Framework which:
   - establishes a national strategy for UK nuclear emergency planning and response
   - requires strong coordination between all parties; and
   - ensures effective communications with local, national and international audiences.
4. Following Japan's worst recorded earthquake in March 2011 and the resulting tsunami, which severely damaged Fukushima Dai-ichi nuclear power site triggering a national and international nuclear emergency, DECC commissioned a report from HM Chief Nuclear Inspector to assess the safety and resilience of UK nuclear facilities.
5. A published progress report on the recommendations made set out a range of areas where arrangements have been further strengthened.

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

The majority of transport operates on a commercial basis, with responsibility for resilience devolved to owners and operators. There are some regulatory means for DfT to control resilience improvements but where these means do not exist the Department has most influence when it can demonstrate the commercial benefit of proportionate and evidence-based resilience planning. This is achieved by the following process:

1. Raising awareness of the biggest risks to transport.
2. Improving understanding of risks, using the best available scientific evidence and operational impact assessments conducted by sector experts.
3. Working with the sector to identify and address the most important resilience capability gaps.
4. Monitoring resilience across the sector, to ensure as far as possible that commercial interests align with the strategic national interest.
5. Ensuring the Department is prepared to respond should any of the risks manifest.

Building Resilience

DfT focus is on risks that the Transport sector has not experienced in recent history and which have the biggest capability gaps. The Department's current priorities are:

Severe coastal flooding – the Department is engaging with ports and local authorities on the east coast of England to raise awareness of this risk and encourage the development of more comprehensive and joined-up response plans
Effusive volcanic eruptions – the Department is seeking to increase scientific understanding of the nature of volcanic gas plumes and their impacts on transport operations
Severe space weather – the Department is engaging with a wide range of national and international stakeholders to determine the impacts of space weather on transport control, navigation and communication systems
Cyber attacks – the Department is developing new guidance to help the sector better manage this risk.

The Department also has ongoing work to enhance resilience to severe weather of all forms, including long term activities to mitigate the impacts of climate change

WATER

SUMMARY: An all risks regulatory framework, mutual aid agreements and high levels of investment continue to strengthen the resilience of the water industry to major risks.

Assessment of existing resilience

1. Irrespective of the risk, water companies are required by law[9] to provide water by alternative means in the event of a failure of the mains supply.
2. Disruption to electricity supplies could result in the loss of mains water and affect the movement and treatment of sewage. A loss of telecoms would impact remote flow management and monitoring systems[10].
3. Water companies have short-term contingency plans in place for power, which include the use of back-up generators. They also continue to develop multiple monitoring systems to reduce impacts of telecoms failure.
4. These resilience efforts are bolstered by an industry-wide mutual aid agreement to enable sharing of emergency equipment and supplies
5. Though it is not a current risk, all companies maintain statutory plans to minimise the impact of a drought.

Building Resilience

6. For the period 2010-2015, Ofwat made £400m available to water companies to improve the resilience of their assets and systems to flooding and other natural hazards. On top of this £470m was made available to enhance the security of assets. Companies have been instructed to once again consider the resilience of assets to major risks in their business plans for 2015-2020.
7. The Water Bill[11] contains a variety of measures to boost the resilience of the water industry, including a primary resilience duty for Ofwat and a power for the Secretary of State to direct water companies to plan for a certain level of resilience. Other measures designed to improve innovation and efficiency should also contribute to enhanced resilience.

[9] Security and Emergency Measures Direction 1998 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85925/semd98.pdf

[10] Principally SCADA (Supervisory Control And Data Acquisition) and other industrial control systems which remotely manage the flow of sewage and treated water, and monitor water quality

[11] Introduced to the House of Commons in June 2013