Cabinet Office

A Summary of the

2014 Sector Resilience Plans

August 2014

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: August 2014

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. As with previous years, 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 fifth round of Sector Resilience Plans and as with previous 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 2014 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
	Telecommunications	Department for Business, Innovation and Skills
Emergency Services	Ambulance	Department of Health
	Maritime & 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 consists of the Telecommunications, Postal and Broadcast sub-sectors. Each has invested proportionately in its resilience to risks including those identified in the National Risk Assessment. The sub-sectors are vulnerable in varying degrees to disruption of other essential services, particularly energy.

Assessment of Existing Resilience

1. Resilience building is driven by a combination of competition, new technologies and the need to meet legislative requirements, standards etc.
2. Contingency plans are in place to manage a broad range of risks. Resilience measures include back up power, service prioritisation and the ability to perform critical functions within existing operations.
3. Where appropriate, organisations have taken expert advice and put in place measures to protect key sites and networks from physical and electronic security threats and natural hazards in line with current risk assessments.
4. Prolonged, widespread disruption to energy supplies and transport networks and damage to infrastructure could disrupt the delivery of services.

Building Resilience

Work continues with partners and expert agencies as follows:

Sector-wide

6. To maintain compliance with legislation and consider the impacts of other potential risks to the sector;
7. To ensure that robust contingency plans are in place to manage emergencies and restore service to customers;
8. 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 telecommunications.

Telecommunications

9. To ensure contingency plans take account of vulnerability to cyber attack and other emerging risks.

Postal

10. To ensure RM contingency plans remain comprehensive and responsive to current and emerging risks.

EMERGENCY SERVICES

SUMMARY: The Emergency Services sector is made up of the Police, Ambulance, Fire & Rescue, and Maritime & 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, including on the Joint Emergency Services Interoperability Programme (JESIP), to improve connectivity of services. A strategic review of the scale of assets in the emergency services sector by CPNI, was initiated 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. A copy can be found at https://www.gov.uk/government/publications/security-policy-framework.

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:

    - Adopt an all risks approach: Under the Utilities Act 2002, Ofgem introduced performance levels for the gas and electricity industry including supply restoration timescales; and Ofgem's 'RIIO' performance standard for network companies' price control periods to ensure efficient investment for continued safe and reliable services.

    - Address specific vulnerabilities: Companies are implementing a large programme of flood protection measures which is due for completion by the early 2020s.

    - Put in place contingency arrangements: Energy companies have worked extensively to put in place contingency plans in the event of disruption due to severe weather related events and to manage staffing in the event of pandemic influenza.

    - 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

2. 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 cyber-attack

    - 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 appropriate levels of resilience to the threats and hazards it faces, reflecting a mature approach to resilience and ongoing investment by firms. The sector, like many sectors, 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. Major risks to the sector include disruption to energy and communications networks, and damage to or destruction of key IT systems and networks.

2. To lessen the impact of electricity and telecoms disruption firms have, for example:

- invested in uninterruptible power supplies and back-up power generators
- built secondary data centres and have access to recovery sites, and
- held industry-wide exercises that included testing the response to and recovery from disruption to telecoms networks.

3. To protect the integrity of IT systems and networks, the sector has worked with expert agencies to:

- address vulnerabilities in the physical integrity of key systems
- 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. However, like many sectors, lengthy or widespread disruption of these networks could pose significant challenges.

Building Resilience

5. The sector will progress existing work to evaluate the impact of severe space weather on systems and networks, and the impacts from disruption to other essential services, in particular communications networks. In addition, in line with the Financial Policy Committee's recommendation in June 2013, HM Treasury and the regulators are working with industry to test and improve the resilience of the sector to cyber attack.

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 there is a widespread dependency 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 the number of supply chains, and the manufacturing and retail options available, coupled with the high degree of substitutability of foodstuffs in the industry make the sector 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. The food retail & wholesale distribution sector has continued to operate at or near to capacity despite the severe winter weather and flooding events experienced from 2010 through to early 2014... 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 build on recent Government sponsored 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. The potential threat to the food and drink industry from food fraud was highlighted in 2013. An independent review of Britain's food system, launched in June 2013, was published in September 2014. More details are available from the Defra and FSA websites. Work is also underway to improve contingency planning and is currently being addressed by expanding the remit of Publicly Available Specification (PAS) 96, "Defending Food and Drink" to include the threat of criminality in the context of fraudulent activity. Plant health has an impact on the food supply and the resilience of food crops and is therefore of importance to the resilience of the food and drink industry. The plant health expert task force published their report in May 2013. A risk register was published in January 2014, a new Chief Plant Health Officer took up the role in April 2014 and a Plant Biosecurity Strategy was published on 30 April 2014. More details are available from the Defra website.

GOVERNMENT

SUMMARY: Government provides a range of essential services through a variety of infrastructure types across the UK. It is vital that these services continue to be delivered throughout disruption. To ensure this is possible, preventative and preparatory measures are continually enhanced against the wide range of risks currently faced by Government to guarantee the sector is as resilient as possible. The sector is currently being reviewed internally to ensure this remains the case.

Assessment of Existing Resilience

1. The Government sector delivers a diverse range of essential functions and public services (for example policy advice, financial management, welfare payments and national emergency responses).
2. Like other sectors, Government has a number of dependencies including power supplies, telecommunications and key staff, the loss or compromise of which are the major risks to the sector.
3. The current assessment of the sector is wide ranging. It goes beyond the sector's registered Critical National Infrastructure assets, and includes vulnerabilities to threats and hazards, including cyber risks.
4. Government promotes a robust security culture, embed risk management principles and undertakes effective resilience planning, all of which are tested and assured on regular basis. This underpins Government's approach to reducing the risk of an incident occurring, ensuring it can respond quickly when things do go wrong and learning lessons effectively for the future. The Security Policy Framework and Guidance on Risk Management provide useful guides on the Government's approach to these areas.
5. Government continues to work with experts, both within the public sector and industry, to better understand and mitigate the risk of both physical and cyber attack as well as supply chain disruption. Work this year will particularly focus on mapping and better understanding cyber resilience and vulnerabilities.

Building Resilience

6. The Cabinet Office is conducting an internal review of the Government sector to ensure best practice is fully adopted across the sector and that current resilience levels match risk appetites.
7. To build on sector-wide efforts to deliver an effective emergency response, departments' resilience efforts should also include work to prevent the occurrence of disruption.
8. Cabinet Office will continue fulfil a co-ordinating role to support departments to ensure central resilience efforts are fully co-ordinated and information is shared effectively across the sector.

HAZARDOUS SITES

SUMMARY: The need to comply with stringent safety and environmental legislation and internationally agreed Conventions promotes 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 and environmental legislation or Conventions promotes a strong safety and working ethos. For example:

- sites governed by the Control of Major Accident Hazard (COMAH) regulations **must,** working with local emergency planners and responders where necessary, put in place **measures** necessary to prevent and respond to major accidents[6]; and

- sites producing certain quantities of particular chemicals are, relevant to the Chemical Weapons Convention (CWC), subject to data monitoring, licensing and national/international inspection. The higher risk sites have been given security advice by Centre for the Protection of National Infrastructure (CPNI) and the National Counter Terrorism Security Office (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 statutory requirements, which enhance resilience efforts.

4. As the challenge set by legislative requirements to firms depends on the type and / or quantity of substance held or produced on site, levels of resilience can legitimately vary across the sector.

5. Previously, sector resilience building has focussed on preventing or minimising casualties following intentional 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.

[6] COMAH safety reports address protection measures against a variety of scenarios including, where appropriate, flooding, earthquakes, high winds and extreme weather. For sites which hold higher hazard substances in certain quantities this process must be captured within the safety report

HEALTH

SUMMARY: Since the publication of the 2013 Health Sector Resilience Plan (HSRP), work has been continuing across the health and social care sector in England to increase its resilience and identify those areas where further improvements are needed to deal with a range of disruptive events.

Assessment of Current Resilience

1. The NHS has good levels of resilience. There are a number of hospitals and services across England and an ability to divert resources from non-essential services in order for life-saving treatment to continue; similar principles apply to the resilience of the ambulance service;

2. The resilience position of the social care sector is more challenging to understand due to the range of services the sector provides as well as the distributed manner in which the services are delivered. However recent challenges such as flooding have demonstrated that there is resilience within the system and that local arrangements are effective in response;

3. Public Health England (PHE) has good preparedness and business continuity arrangements;

4. NHS Blood & Transplant (NHSBT) is considered to be in a good position in terms of its resilience. By the nature of its day to day business it routinely deals with surges in the demand for blood.

Building Resilience

Throughout 2014, health organisations in England will be working to ensure that they have their own plans based on national and local risk assessments, and also joint plans and processes related to key dependencies, infrastructure, the workforce and the supply chain. Lessons identified from real incidents, notably the winter 2013-2014 floods will be captured and shared. In particular:

5. Department of Health (DH) will be working across the health sector to consider resilience to fuel shortages as part of the Department of Energy and Climate Change-led work to review the National Emergency Plan for Fuel (NEPF);

6. DH will consider recommendations from the independent review conducted in 2013 into the resilience of contingency arrangements for the NHS supply chain for medical devices, consumables and pharmaceuticals;

7. DH will work with the Department for Communities and Local Government and professional organisations to take forward any lessons identified after the winter 2013-2014 flooding for improving how the residential care sector provides support in any future events;

8. Working with NHS England, PHE will develop the pilot National Resilience Capabilities Assessment (NRCA) to identify and assess the capability to respond to a mass casualty event to be completed during 2014.

9. DH, NHS England and PHE are also working closely with colleagues in Cabinet Office to consider the health response to an effusive volcanic eruption;

10. DH Emergency Preparedness Resilience and Response (EPRR) and Communications teams are working together to develop a process for ensuring effective, clear, coordinated and timely communications across the health sector in the event of an emergency.

CIVIL NUCLEAR

SUMMARY: The nuclear sector's resilience to major risks is ensured through high build standards, a stringent regulatory regime, and effective governance.

Assessment of Existing Resilience

1. The first annual Nuclear Chief Inspector's Report from the nuclear regulator, ONR, concluded that the UK's operating civil nuclear reactors defueling and decommissioning sits and defence related sites meet the safety standards required.

2. 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.

3. Infrastructure owners are required to comply with national standards regulating the safety and security of nuclear licensed sites.

    - **Security**. The UK nuclear sites have an up-to-date, approved security plan and meet the standards of security required by the regulator.
    - **Safeguards:** UK obligations concerning the reporting and/or publication of safeguards related information were met, and Euratom and IAEA reporting on their verification activities in respect of civil nuclear material in the UK during 2012 concluded there had been no diversion of material from peaceful use.

Building Resilience

4. 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.

5. 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.

6. 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, established that the UK nuclear sector has high safety standards. The sector is now responding to the challenge of 'beyond the reasonably forseeable' risk events to ensure resilience in the face of outlying events, such as was witnessed at Fukushima.

TRANSPORT

SUMMARY: The Transport sector comprises the road, aviation, rail and maritime sub-sectors. The majority of transport operates on a commercial basis, with responsibility for resilience devolved to owners, operators and regulators. DfT works closely with industry stakeholders to develop a common assessment of risks and ensure that proportionate and cost-effective mitigations are in place.

Assessment of Existing Resilience

1. The scale and exposed nature of the transport network makes it vulnerable to some significant risks, such as severe weather. However, multi-agency emergency planning, investment in technological solutions and the interconnected nature of its networks, all lend resilience to the sector.

Building Resilience

2. 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:

    - **Climate change & severe weather –** following the severe weather of winter 2013-14, the Department has commissioned a review of risks to transport from climate-driven events such as storms, flooding and heatwaves. (https://www.gov.uk/government/groups/review-of-the-resilience-of-the-transport-network-to-extreme-weather-events-expert-panel)
    - **Highway repairs -** in response to severe weather over several winters, the Department has significantly increased the funding available to local authorities in FY14-15 for road repairs (https://www.gov.uk/government/news/councils-urged-to-apply-for-168-million-pothole-repair-fund)
    - **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.

3. The Department also has ongoing work to update its:

    - Risk assessment methodology and risk register
    - Assessment of resilience of critical national transport infrastructure
    - Response procedures for major transport incidents

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[7] to plan 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 sewerage. A loss of telecommunications would impact remote flow management and monitoring systems[8].

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 not a current risk, all companies maintain statutory plans to minimise the impact of a drought.

Building Resilience

6. The Water Act 2014 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.

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

[8] 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