Cabinet Office

Summary of the

2016

Sector Security and Resilience Plans

Produced by:

Cabinet Office
35 Great Smith Street
LONDON
SW1P 3BQ

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

Contact:

Civil Contingencies Secretariat

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

Publication date: November 2016

INTRODUCTION

1. Sector Security and Resilience Plans set out the resilience of Critical Sectors to the relevant risks identified in the National Risk Assessment.[1] The Plans are placed before Ministers each year to alert them to any perceived vulnerabilities, with a programme of measures to improve resilience where necessary.

2. The UK's Critical Infrastructure is defined by the Government as: "*Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:*

    a) *major detrimental impact on the availability, integrity or delivery of essential services – including those services, whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or*

    b) *significant impact on national security, national defence, or the functioning of the state."*

3. There are 13 UK Critical Sectors: Chemicals; Civil Nuclear; Communications; Defence; Emergency Services; Energy; Finance; Food; Government; Health; Space; Transport; and Water (see Table 1).

4. Working, where appropriate, with infrastructure owners and regulators, the Government Departments responsible for the 13 Critical Sectors are required to produce Sector Security and Resilience Plans on an annual basis. The process is coordinated by the Civil Contingencies Secretariat (based in the Cabinet Office).

5. This is the seventh round of Sector Security and Resilience Plans and as with previous Plans, they allow departments to review the resilience of their most important infrastructure to all risks (threats, cyber and hazards). As identified in the National Risk Register of Civil Emergencies 2015, cyber security is a particular challenge as attacks are increasingly being carried out on an industrial scale. Some 90% of large corporations and 74% of small businesses reported an information security breach in 2015. On average, more than 33,000 malicious emails are blocked at the Gateway to the Government Secure Intranet (GSI) every month, while around 90 sophisticated attacks are carried out against industry and government per month.

6. Owing to their sensitive nature, individual plans are classified. This document presents an unclassified summary of the 2016 Sector Security and Resilience Plans.

[1] The National Risk Assessment is the main document Government uses to assess the major threats (malicious terrorist attacks); hazards (non- malicious risks such as human and animal diseases, industrial accidents and industrial action, natural hazards such as flooding and drought) and cyber threats the UK could face in the next five years. A public summary – National Risk Register of Civil Emergencies 2015 is available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf

STANDARDS

7. Standards of various types help to assure the readiness and resilience of different sectors. Some of these are sector-specific performance standards which define the expectations of government, regulators or industry associations. A second type are National and International Standards. In the UK, the British Standards Institution (BSI) is the National Standards Body, and BSI works closely with the International Standards Organisation (ISO) in developing or adopting International Standards for use in the UK. Standards are simply an agreed way of doing something; they capture current good practice through trusted processes involving relevant stakeholders.

8. In some contexts Standards are an alternative to regulation, in other contexts they support regulation. A key feature of such Standards is that they are created and maintained by communities of practice and reflect good practice, drawing on the expertise of business and industry, consumers, government, innovators and others. They can be agreed specifications, recommendations, guidelines or principles, and different types of Standards are suited to different contexts. Products and technical processes are typically subject to specification standards, while wider governance aspects of business are typically subject to guidelines or codes of practice.

9. Critical Sectors make extensive use of BSI and ISO specification Standards, for instance in relation to building standards, environmental performance and Personal Protective Equipment (PPE). A range of guidance Standards in relation to risk, security and crisis management, corporate governance and organisational resilience are also relevant to Critical Sectors and will be promoted as complements to other sources of formal guidance where they drive rigour and coherence in resilience activities. These include BS65000 Guidance for Organisational Resilience (published in November 2014), which provides an overview of resilience, describing the foundations required and explaining how to build resilience.

10. Standards under development include guidance on the validation and assurance of resilience arrangements and capabilities, a framework that will be of mutual interest to government, regulators, sector operators and other resilience partners.

TABLE 1: CRITICAL SECTORS, ASSOCIATED SUB-SECTORS AND LEAD GOVERNMENT DEPARTMENTS

Sector	Sub –Sector(s)	Sector Resilience Lead [2]
Chemicals		Department for Business, Energy and Industrial Strategy
Civil Nuclear		Department for Business, Energy and Industrial Strategy
Communications	Broadcast	Department for Culture, Media and Sport
	Telecommunications	
	Internet	
	Postal	Department for Business, Energy and Industrial Strategy
Defence		Ministry of Defence
Emergency Services	Ambulance	Department of Health
	HM Coastguard	Department for Transport
	Fire & Rescue	Home Office
	Police	Home Office
Energy	Electricity	Department for Business, Energy and Industrial Strategy
	Gas	
	Oil	
Finance		HM Treasury
Food		Department for Environment, Food and Rural Affairs
Government		Cabinet Office
Health		Department of Health
Space		Department for Business, Energy and Industrial Strategy
Transport	Aviation	Department for Transport
	Ports	
	Rail	
	Road	
Water		Department for Environment, Food and Rural Affairs

Government's approach to building Infrastructure Resilience [3]

[2] 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 2015 Sector Security and Resilience Plans covered the entirety of the UK.

[3] 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

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.

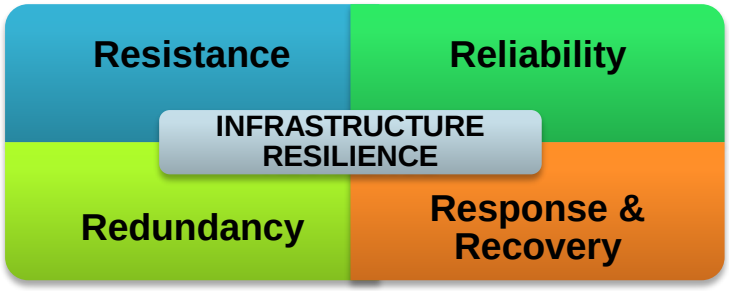

Figure1: The components of infrastructure resilience

- **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.

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.

CHEMICALS

SUMMARY: The chemicals sector complies with stringent safety and environmental legislation. 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 their use in explosive devices, work continues to identify and review the resilience of those sites whose activities support the delivery of essential services. Government has recently designated Chemicals a 'Critical Sector'.

Assessment of Existing Resilience

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 subject to the Control of Major Accident Hazard (COMAH) regulations must take all necessary measures to prevent major accidents involving dangerous substances and limit the consequences to people and the environment of any major accidents[4] which do occur, e.g. by working with local emergency planners and responders to prepare suitable emergency plans;
- sites producing certain quantities of particular chemicals relevant to the Chemical Weapons Convention (CWC) are subject to data monitoring, licensing and national/international inspection.

At the local level, to support site protection and incident response, relevant emergency planning authorities work with infrastructure owners to maintain emergency plans and a list of hazardous substances on-site.

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

Previously, sector resilience building has focussed on preventing or minimising casualties following a chemical release and preventing their use in explosive devices. However, the impact of other risks on some sites could disrupt the flow of chemicals to other critical sectors, thereby disrupting the provision of services to the public.

Building Resilience

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.

[4] 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

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

The latest annual Nuclear Chief Inspector's Report from the independent nuclear regulator, the Office for Nuclear Regulation, concluded that the UK's civil nuclear sector meets the safety and security standards required to operate.

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.

The civil nuclear industry is required to comply with the following national standards:

- **Safety**. UK nuclear sites have legal responsibility for ensuring nuclear safety on their sites and are held to account by a robust licensing system.
- **Security**. All UK nuclear sites have an up-to-date, approved Nuclear Site 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[5] and IAEA[6] reporting on verification activities in respect of civil nuclear material in the UK during 2014 and 2015 respectively concluded there had been no diversion of material from peaceful use. The Euratom report for 2015 has not yet been issued.

Building Resilience

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] European Atomic Energy Committee

[6] https://www.iaea.org/

COMMUNICATIONS

SUMMARY: The Communications sector comprises telecommunications, internet, postal services and broadcast. The sector has invested proportionately in its resilience to risks. Like many other sectors, it is vulnerable to prolonged and widespread disruption to services such as fuel and energy, however levels of resilience are generally good and industry has contingency plans in place to handle a wide range of risks.

Assessment of Existing Resilience

Major risks to the sector include disruption to energy and fuel as well as damage to key elements of national infrastructure.

Resilience building is driven by a combination of competitive pressures, new technologies and the need to meet legislative requirements, licences or standards.

Resilience measures include back up power generation, service prioritisation and the take up of advice to protect key sites and networks from natural hazards as well as physical and electronic security threats.

Industry has put in place contingency plans to handle a wide range of risks and there are regular exercise programmes in place to test these plans.

Building Resilience

The sector continues 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.

More specific priorities include:

- **Telecoms & Internet; Broadcast –** To work with industry to assess the risk posed to the sector by cyber-attack.
- **Postal Services –** To work with Royal Mail to maintain robust contingency and resilience plans in response to key risks to the national network.

DEFENCE

SUMMARY: Defence officially became a sector in 2014, previously part of the Government Sector. MOD is the Lead Government Department and is also directly responsible for sites that house Defence owned Critical National Infrastructure. MOD may be called upon to support the other critical sectors at times of emergency or significant disruption.

Assessment of Existing Resilience

Defence protects the national security and independence of the UK, operating from a wide variety of sites and using a wide variety of capabilities and equipment. Defence has a number of dependencies, including power supplies, telecoms and key personnel.

The current assessment of the sector is wide ranging. It goes beyond the sector's CNI assets, and includes its vulnerabilities to threats and hazards, including cyber risks.

Defence promotes a robust security culture, compliant with HMG Security Framework and working with other departments to maximise the security of our sites, personnel and equipment.

MOD has sites across the UK and is exposed to the range of local weather and environment hazards.

MOD's BC policy is in line with the Government Security Framework, which mandates BCMS consistent with the British Standard 22301. This ensures that business units can maintain critical functions despite disruptive events.

Building Resilience

The SDSR reinforced MOD's role in supporting UK resilience.

This is the first SSRP Defence has had to produce; lessons identified will build on this to develop more coherent processes.

Head Office will continue to fulfil a coordinating function, to support TLBs (and TFs) to develop their understanding of the resilience requirements of their business and critical functions best – to understand their resilience requirements.

MOD is actively addressing physical resilience requirements as part of broader infrastructure improvements driven by a Strategy for Defence Infrastructure.

EMERGENCY SERVICES

SUMMARY: The Emergency Services sector is made up of the Police, Ambulance, Fire and Rescue, and Maritime and HM Coastguard. 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

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.

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, radio communications and local solutions.

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 backup power supplies;
- the ability to divert emergency calls between call centres;
- complied with the HMG Security Policy Framework[7];
- 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

The emergency services continue to work together to improve resilience, including:

- the Joint Emergency Services Interoperability Programme (JESIP), currently being reviewed by an Her Majesty's Inspectorate of Constabulary-led tri-service team to assess to degree to which this has been embedded; and
- the Emergency Services Mobile Communications Project (ESMCP) which is seeking a replacement for Airwave to further improve connectivity of services. A strategic review of the scale of assets in the emergency services sector by Centre for the Protection of National Infrastructure (CPNI) was initiated 2013.

[7] 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 supply sector is made up of upstream oil and gas, downstream oil and gas, and electricity. Although infrastructure types and business environments differ, each sub-sector has invested proportionately to build resilience to major risks.

Assessment of Existing Resilience

Major risks to the energy sector include storms and gales, flooding, accidents, and loss of key staff. Government, regulators and the supply industry work together to ensure risks to supply are appropriately mitigated.

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, based on regular risk assessments and reviews of resilience problems that have occurred in the UK and elsewhere: for example, companies have been implementing a large programme of flood protection measures over recent years, 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 flu and other risks.

Building Resilience

Priorities include:

- Electricity: Implementing a three digit emergency phone number for reporting power disruption.

- Energy 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.

- Energy Sector Flood Resilience: Continuing assessment of flood risks to energy assets and flood protection enhancement programmes.

FINANCE

SUMMARY: Over the past year, the finance sector has made good progress in improving its resilience to a range of threats and hazards, reflecting a mature approach to resilience and ongoing investment by firms. However, the sector continues to face risks, in particular from cyber-attacks. Over the next year, HM Treasury, the Bank of England and the Financial Conduct Authority will deliver a comprehensive work programme to continue to build resilience to cyber and operational risks in the finance sector.

Assessment of Existing Resilience

Risks to the finance sector include the potential disruption caused by cyber-attacks, IT failures, personnel and physical security risks. There is also a potential impact on the finance sector from disruption to other sectors such as energy and telecoms.

Over the last year, HM Treasury, the Bank of the England, the Financial Conduct Authority (FCA), and the Prudential Regulatory Authority (PRA) have worked with the finance sector to test its resilience to these risks, and identify areas for further improvement. This has included the Bank of England's CBEST cyber vulnerability testing programme, and the FCA and PRA's Dear Chairman Exercise II, which tested the resilience of the seven largest UK deposit-takers to IT failure.

HM Treasury, the Bank of England and the Financial Conduct Authority have refined and tested their own incident response frameworks, including through the 'Resilient Shield' exercise in November 2015, which tested the ability of the UK and US to cooperate and respond effectively if faced with an international cyber-incident in the finance sector.

Building Resilience

Over the next year, HM Treasury, the Bank of England and the Financial Conduct Authority will continue to work together to deliver improvements in the resilience of the finance sector. We will continue to test the resilience of the sector, and refine and improve our own response frameworks, and the tools we have to deliver improved resilience. We will further analyse the potential impacts on the finance sector, including from severe space weather, as well as disruption to other essential services, in particular communications and power networks. We will continue to maintain strong links with international partners.

We will work closely with the new National Cyber Security Centre (NCSC). As announced in March, one of the first tasks of the NCSC will be to work with the Bank of England to produce advice for the financial sector for managing cyber security effectively.

We will continue to work closely with the finance sector, including through the senior Cross Market Operational Resilience Group (CMORG), chaired by the Bank of England.

FOOD

SUMMARY: The UK food sector has a highly effective and resilient food supply chain, owing to the size, geographic diversity and competitive nature of the industry. Although there is recognised dependency on other critical services such as fuel, energy, transport and communications the resilience of the sector has been demonstrated by the response to potentially disruptive challenges in recent years.

Assessment of Existing Resilience

Like many industries the food sector operates just-in-time supply chains which require sophisticated logistics operations and contingency plans to respond rapidly to potential disruption. The industry remains highly resilient owing to the capacity of food supply sectors and the high degree of substitutability of foodstuffs.

This resilience has been demonstrated in the response to events such as the 2015 flooding, and disruption to cross-channel transportation, the 2009 H1N1 Pandemic, the 2010 Icelandic volcanic ash clouds, the 2012 potential industrial action by fuel tanker drivers and severe winter weather experienced over the years 2010–2014.

More recently, the food distribution sector continued to operate without significant disruption during the severe winter weather experienced in 2013-2014.

Building Resilience

Government and the sector will continue to work together to ensure the resilience of food supply. This will include building on recent research into the resilience of food supply to respond to and recover from maritime transport disruption resulting from a major coastal flooding event, building resilience in supply chains to extreme weather events, and providing good practice guidance on cyber security.

GOVERNMENT

SUMMARY: Government provides a range of essential services through various infrastructure types across the UK. Cabinet Office and the lead departments have developed a sound understanding of the risks the sector faces. A broad range of measures are in place, that are kept under regular review to meet developing threats and ensure the sector is as secure and resilient as possible. Cabinet Office will continue to fulfil a coordinating role to support departments to ensure central security and resilience efforts are appropriately directed and information is shared across the sector.

Assessment of Existing Resilience

Major risks identified across the sector include malicious cyber activity, acts of terrorism, espionage and other criminal activity, as well as natural hazards and technical failures. The breadth of these concerns requires a range of security and resilience measures in response.

Preventing and mitigating the impact of Cyber incidents remains a significant challenge for the Government sector, and substantial work has been carried out as part of the National Cyber Security Strategy. To ensure that the UK remains at the forefront of actively preventing and tackling malicious behaviour, the Government has committed further investment in cyber security and has brought expertise together in the National Cyber Security Centre.

Government is currently reviewing how security is delivered within departments to ensure we promote a robust security culture and are best able to respond to both current and future threats. Improvements have already been made by introducing shared service models which provide consistent and high standards of expertise; these include a standardised single vetting provider and a move to delivering physical security through a shared estates strategy.

Building Resilience

Security in Government will continue to evolve and a rolling programme of assessment is in place to identify new vulnerabilities as well as measures to further strengthen mitigations against the risks and hazards this sector faces. Departments will be accountable for ensuring they have effective personnel, physical and cyber security to defend against hostile foreign intelligence activity to agreed standards. Improvements in working with the commercial sector will help to deliver increased security assurance from suppliers.

Cabinet Office continues to engage as appropriate with Devolved Administrations to ensure joined up and mutually supportive programmes, and to ensure that resources can be prioritised and expertise shared

HEALTH

Assessment of Existing Resilience

The NHS and Public Health England (PHE) have good levels of resilience and business continuity 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. NHS Blood & Transplant (NHSBT) routinely deals with surges in the demand for blood.

Although there is resilience within the system and local arrangements are effective in response, the social care sector is more challenging to understand. Continuous further work is undertaken with local government, the provider and voluntary sector representatives to consider emerging issues regarding emergency planning, communication and information flows.

Building Resilience

Throughout 2016-17, health organisations in England will continue 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, utilities, the workforce and the supply chain. Lessons identified from real incidents, will be captured and shared. In particular:

- Department of Health (DH) will be working across the health sector to consider resilience to prolonged electricity supply disruption and fuel shortages and the ongoing National Flood Resilience Review (NFRR).

- National supply resilience strategies for critical medical devices and clinical consumables continue to be developed and implemented.

- DH, NHS England and NHS BT will continue to progress work on the findings of the Mass Casualties National Capabilities Risk Assessment (NCRA).

Response to Incidents

- After a period when the British Medical Association (BMA) has been in formal dispute with employers and the Government, the BMA agreed to suspend industrial action.

- Following the December 2015 storms, the health and social care sectors performed well in delivering services and supporting local response and recovery efforts. However difficulties were encountered following disruption to electricity, transport and telecommunication links.

- Over the last 12 months the DH has activated two separate National Supply Disruption Responses and further 3 significant supply disruption events which did not require a national response. Due to actions across the health system, no adverse impacts on patient care were reported in any of these incidents.

- Health and Social Care Information Centre (HSCIC) launched CareCERT last year, to provide advice and guidance to the health sector to respond to cyber security threats and to protect from malicious attacks.

- PHE responded to twelve Level 2 incidents (across multiple PHE Centres), and six Level 3 and Level 4 incidents requiring national coordination (including the Ebola response).

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 and operators. The Department for Transport (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

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 engineering and technological solutions, and the interconnected nature of transport networks all lend resilience to the sector.

Building Resilience

DfT's focus is on risks which have the highest impact or which have the biggest capability gaps. The Department's current priorities include:

- **Security:** The Department engages with industry, cross-Government colleagues and international partners to put in place effective and proportionate mitigation measures to protect the Transport network.

- **Incident response**: The Department works with the intelligence community, other departments, local responders and industry and has an ongoing programme of work to improve our response procedures.

- **Cyber-attacks:** The Department has an active cyber security programme, working closely with industry as well as Government and international partners to identify and mitigate cyber risks and vulnerabilities across all transport modes.

- **Climate change & severe weather:** The Department is working to identify local road networks in England that are at risk of flooding to provide an assessment of the impact of roads/bridges on communities if they are unavailable. This work includes looking at isolated communities, critical or vulnerable local highway infrastructure and diversionary routes. This is part of the wider Government review on flood preparedness put in place following the 2015/16 winter floods.

- **Industrial action:** Strike action in the transport sector can have a major and adverse impact on the ability of very large numbers of people to get to their place of work or education, not to mention impacts on other important journeys. This is particularly unfair when it goes ahead on the support of only a small proportion of union members. The Trade Union Act will ensure that strikes are only ever the result of a clear and positive mandate from union members.

- **Severe space weather:** We are engaging with a number of government and industry stakeholders to build awareness and plan for the impacts of space weather on transport control, navigation and communication systems.

As part of our regular resilience work, DfT:

- has a specific engagement programme with industry on winter weather resilience;
- delivers targeted research programmes to provide evidence to support policy development for secure and resilient transport;
- maintains collaborative relationships with the transport industry

WATER & SEWERAGE

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 disruptive events.

Assessment of existing resilience

Irrespective of the risk, water companies are required by law to plan to provide water by alternative means in the event of a failure of the mains supply.

The piped water supply system is generally resilient to the loss of individual facilities, and there is a widespread ability to reroute supplies from other parts of networks.

However disruption to electricity supplies or widespread flooding could result in the loss of mains water and affect the movement and treatment of sewage. Water companies have contingency plans in place which include the use of back-up generators, temporary flood defences and, where piped supplies cannot be maintained, the provision of bottled water or bowsers.

Emergency response is bolstered by industry-wide and local mutual aid agreements to enable the sharing of resources between companies which has recently been expanded to include response to flooding.

All companies maintain statutory plans to minimise the impact of drought.

Further work is being undertaken with the companies to improve cyber security and review the framework for protective security in the sector.

Following the publication of the National Flood Resilience Review companies are also improving the resilience of key water infrastructure to flooding and ensuring data is shared with Local Resilience Forum partners.