Cabinet Office

Summary of the

# 2015-16

# Sector 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: April 2016*

## INTRODUCTION

1. Sector 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. Chemicals, Civil Nuclear, Defence and Space are newly designated 'Critical Sectors'. Chemicals (formerly Hazardous Sites) and Civil Nuclear have previously produced Sector Resilience Plans. Defence and Space are developing their first Sector Resilience Plans, for publication in 2016.

[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 animals 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

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

6. This is the sixth 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, 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.

7. Owing to their sensitive nature, individual plans are classified. This document presents an unclassified summary of the 2015 - 2016 Sector Resilience Plans.

## STANDARDS

8. 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.

9. In some contexts they 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 Standard 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.

10. 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.

11. 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, Innovation and Skills |
| **Civil Nuclear** | | Department of Energy and Climate Change |
| **Communications** | Broadcast | Department for Culture, Media and Sport |
| | Telecommunications | |
| | Internet | |
| | Postal | Department for Business, Innovation and Skills |
| **Defence** | | Ministry of Defence |
| **Emergency Services** | Ambulance | Department of Health |
| | HM Coastguard | Department for Transport |
| | Fire & Rescue | Department for Communities and Local Government |
| | Police | Home Office |
| **Energy** | Electricity | Department of Energy and Climate Change |
| | Gas | |
| | Oil | |
| **Finance** | | HM Treasury |
| **Food** | | Department for Environment, Food and Rural Affairs |
| **Government** | | Cabinet Office |
| **Health** | | Department of Health |
| **Space** | | Department for Business, Innovation and Skills |
| **Transport** | Aviation | Department for Transport |
| | Ports | |
| | Rail | |
| | Road | |
| **Water** | | Department for Environment, Food and Rural Affairs |

[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 2015-16 Sector Resilience Plans covered the entirety of the UK.

## Government's approach to building Infrastructure Resilience [3]

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.

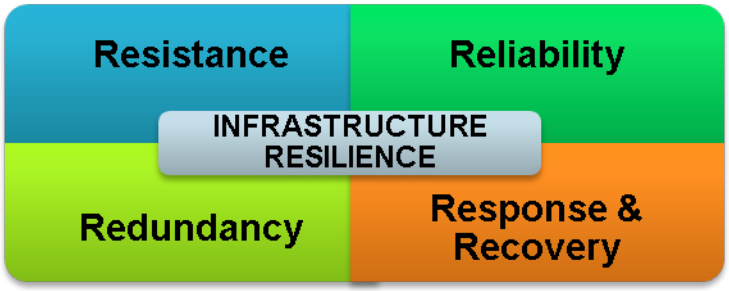


Figure1: The components of infrastructure resilience

- **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.

[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

## CHEMICALS

**SUMMARY:** The chemicals sector needs to comply with stringent safety and environmental 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 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 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[4]; and
- 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.

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

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 owners to maintain emergency plans and a list of hazardous substances on-site.
- IAEA reporting on verification activities in respect of civil nuclear material in the UK during 2014 concluded there had been no diversion of material from peaceful use. Euratom reporting for 2013 also concluded no diversion - their report for 2014 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.

## 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 good and there are inevitable limits to how far vulnerability to very severe events can be reduced.

### 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 cyber security threats.

Telecoms and postal services: 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 –** 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.

## 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 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

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 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.

## ENERGY

**SUMMARY:** The Energy sector is made up of 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

Major risks to the energy sector include all types of flooding (including coastal flooding), storms and gales, and absence 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'[6] 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 ongoing, but reducing, risk of disruption.

### 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.

[6] Ofgem's (Revenue=Incentives+Innovation+Outputs) performance-based model for setting network companies' price controls over 8 year periods.

## 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.

### Assessment of Existing Resilience

Major risks to the sector include disruption to energy and communications networks, and damage to or destruction of key IT systems and networks.

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.

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 resilience of these systems to cyber attack and
- complete personnel security checks.

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

The sector continues to progress with 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 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 2007 flooding, the 2009 H1N1 Pandemic, the 2010 Icelandic volcanic ash clouds, the 2012 threatened industrial action by fuel tanker drivers and severe winter weather experienced over the years 2010–2011.

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, and building resilience in supply chains to extreme weather events.

## GOVERNMENT

**SUMMARY:** Government provides a range of essential services through various infrastructure types across the UK. Cabinet Office, HMG's corporate centre, and 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 acts of terrorism, cyber attack, 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.

Like other sectors, Government has a number of key dependencies, notably: energy supply, telecommunications and key staff, the loss or compromise of which are major risks to the sector. Cabinet Office co-ordinates cross-sector work to mitigate these vulnerabilities.

Government promotes a robust security culture, embeds risk management principles and undertakes effective resilience planning, all of which are tested and assured on regular basis. The Security Policy Framework and Guidance on Risk Management provide useful guides on the Government's approach to these areas.

Government continues to work with experts; both within the public sector and industry, to better understand and mitigate its priority risks, and promote resilience across its supply chain. Work this year will focus on better understanding current levels of resilience to cyber attack and how these can be improved.

- the ability to divert emergency calls between call centres;

### Building Resilience

A recent Cabinet Office review of the Government sector has added to our understanding of key assets across the sector. This work is also baselining existing protections and identifying measures to further improve mitigations against the risks and hazards this sector faces. Departments will be expected to prioritise resilience, at both Board and asset level.

Cabinet Office is working with Devolved Administrations to ensure joined up and mutually supportive programmes, and to ensure that resources can be prioritised and expertise shared.

## HEALTH

**SUMMARY:** The NHS has good levels of resilience 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.

### Assessment of Existing Resilience

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

**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. Further work is underway with local government, the provider and voluntary sector representatives to consider emerging issues regarding emergency planning, communication and information flows.

### Building Resilience

Throughout 2015-16, 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, the workforce and the supply chain. Lessons identified from real incidents, notably the 2013-14 flooding, 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.
- National Supply Disruption Response guidelines were issued in Dec 2014. DH has initiated a pilot project to develop and test an on-line supply risk assessment process.
- DH, NHS England and NHS BT will be meeting in spring 2015 to progress work on the findings of the Mass Casualties National Resilience Capabilities Assessment (NRCA).

### Ebola Virus Disease (EVD) Response

An important stress on health resilience has been the response to the large outbreak of Ebola in West Africa.

- The UK is leading the international response in Sierra Leone in order to halt the disease in West Africa, including building treatment centres, testing laboratories and deployment of UK volunteers.
- The UK continues to lead the way on the development of a vaccine.
- The NHS has a country-wide network of infectious diseases consultants, specialist beds and isolation facilities.

**As of 19 October 2015, there have been 3 cases treated in the UK, all in health care workers who had contracted the disease in Sierra Leone. There has been no community transmission of the disease in the UK.**

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

### Building Resilience

DfT focus is on risks which have the highest impact or the biggest capability gaps. Our current priorities include:

- **Security** – We engage with industry, cross-Government colleagues and international partners to put in place effective and proportionate mitigation measures to protect the Transport network.

- **Incident response** – We work with the intelligence community, other departments, local responders and industry and have an ongoing programme of work to improve our response procedures.

- **Cyber-attacks** – We are developing new guidance to help the sector better manage this risk and working more closely with industry to understand vulnerabilities and develop an integrated programme to deliver improvements.

- **Climate change & severe weather** – The Transport Resilience Review published in June 2014 reviewed the risks to transport from climate-driven events such as storms, floods and heatwaves. Both DfT and industry have taken its recommendations forward. This remains a high priority for DfT due to the substantial impact and likelihood of severe weather.

- **Industrial action** – This can cause significant disruption to the travelling public across all transport sub-sectors. We are working with industry and lead government departments to understand the risk and mitigate the impact on the public and wider industry.

- **Severe space weather** – We are engaging with a wide range of national and international stakeholders to determine 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; and

- delivers targeted research programmes to provide evidence to support policy development for secure and resilient transport.

## 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.

Disruption to electricity supplies could result in the loss of mains water and affect the movement and treatment of sewerage. A loss of telecoms could impact remote flow management and monitoring systems.

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.

These resilience efforts are bolstered by an industry-wide mutual aid agreement to enable sharing of resources between companies.

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

### Building Resilience

Priorities include:

**Cyber Security:** To better understand the vulnerability of the water industry to cyber-attack, the potential consequences of such an attack, and the options for mitigating the risks.

**Re-zoning:** To build a better understanding of the capabilities within the industry to re-route water supplies from other parts of water networks (“re-zoning”) in the event of a loss of one or more water supply assets, and of the numbers of people potentially left without supply after all re-zoning options had been implemented.

**Power loss:** To build a deeper understanding of the resilience of the water industry against significant power loss.

**Flooding:** To build a wider knowledge-base of the resilience of water supply assets to flooding across the industry.