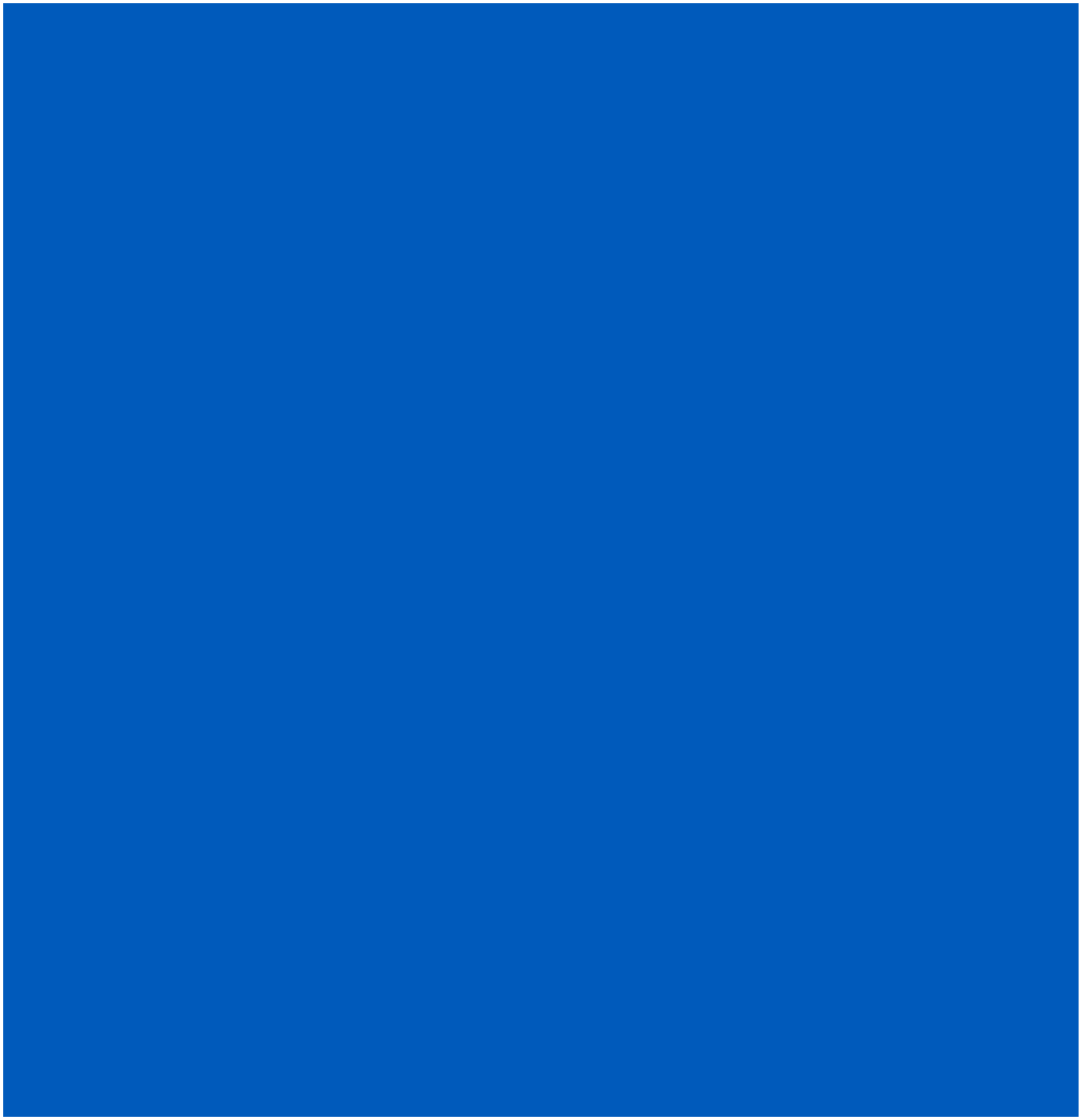
Cabinet Office

Public Summary of Sector Security and Resilience Plans

2017



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: December 2017

Contents

Introduction

Securing the UK's most essential public and private sector services against wide-ranging threats and hazards forms an integral part of HMG's National Security Strategy.[1]

The Cabinet Office commissions Lead Government Departments (LGDs) responsible for the UK's 13 critical sectors to produce annual Sector Security and Resilience Plans (SSRPs), which describe:

- LGDs' approaches to critical sector security and resilience;
- their assessments of significant risks to their sectors;
- their approach to security and resilience in the UK; and
- activities they plan to undertake to mitigate and respond to those risks.

The SSRPs are produced by officials in the LGDs, in consultation with Infrastructure owners and operators, regulators and Government agencies, before being signed-off by Ministers.

The genesis of the SSRPs can be found in a report produced by Sir Michael Pitt, 'Learning Lessons from the 2007 Floods'.[2]

The Sector Resilience Plans (SRPs) were originally intended to focus on resilience to flooding. In 2010 the scope of the Plans was expanded to cover all hazards and security threats relevant to each sector and they were renamed 'Sector *Security* and Resilience Plans (SSRPs)'. Henceforth, the SSRPs have included information on physical, personnel and cyber security as well resilience to hazards.

The full SSRPs are classified documents as they contain sensitive security information. However, each year Government publishes unclassified summaries of the Sector Security and Resilience Plans to provide members of the public with information on activity being undertaken in each sector to improve security and resilience.

This document sets out the public summaries of the 2017-18 SSRPs, with the intention of promoting public understanding of the risks to the UK's critical sectors and measures being taken by HM Government to mitigate those risks.

To provide some context for the reader, this document also describes:

- what we mean by 'Critical National Infrastructure' and 'critical sectors';
- significant threats and hazards that can affect our critical sectors;
- our approach to security and resilience in the UK; and
- responsibilities of different organisations for critical sectors' security and resilience.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

[2] http://webarchive.nationalarchives.gov.uk/20100702222706/http://archive.cabinetoffice.gov.uk/pittreview/_/media/assets/www.cabinetoffice.gov.uk/flooding_review/pitt_review_full%20pdf.pdf

Critical National Infrastructure

National Infrastructure consists of those facilities, systems, sites, information, people, networks and processes necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential dangers they could pose to the public in the event of an emergency (civil nuclear and chemicals sites for example).

There are some parts of the National Infrastructure system that are judged to be critical to the functioning of the country. This Critical National Infrastructure (CNI) includes buildings, networks and other systems that are needed to keep the UK running and provide the essential services upon which we rely (e.g. energy, finance, telecoms and water services). It also includes Infrastructure, which if disrupted could have a significant impact on our national security collectively, national defence, or the functioning of the state. A significant proportion of our CNI is privately owned.

The UK's Critical Infrastructure is defined by the Government as:

'Those critical elements of Infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life.'

In the UK there 13 Critical National Infrastructure Sectors:

Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water.

Several sectors also have defined 'sub-sectors'; Emergency Services for example can be split into Police, Ambulance, Fire and Rescue Services, and Her Majesty's Coastguard.

Threats and Hazards

The Government's assessment of threats and hazards to CNI is based on a continuous cycle of learning lessons from real world events, drawing on evidence and improving the ways in which we calculate the likelihood and potential impacts (consequences) of threats and hazards.

Understanding the range of threats and hazards facing our CNI is crucial to ensuring security measures and mitigations are proportionate, effective and responsive. The UK's CNI faces various threats and hazards.

Threats

National Infrastructure could be targeted by hostile states, cyber criminals, terrorists or criminals for the purposes of disruption, espionage and/or financial gain.

For example, the Centre for the Protection of National Infrastructure (CPNI) judges that National Infrastructure sectors represent core strategic interests for foreign intelligence services, whose targeting against the sectors is likely to include espionage for economic, political, military or commercial gain.

While the current terrorist threat to the National Infrastructure can be characterised as generally limited and often aspirational, the transport sector continues to face enduringly high levels of threat from international terrorism. In addition, the Emergency Services and Defence sectors (specifically police and military personnel), also face a high level of threat from both international terrorism and Dissident Republic groups in Northern Ireland. With the continual diversification of the threat, the ambition and capability of terrorist groups to target UK Infrastructure is likely to continue to evolve.[3]

The National Cyber Security Centre (NCSC) judges there is also a growing cyber threat. There are now more devices connected to the internet than ever before, and with the growth of our dependence on technology comes increased risk. We know there are hostile states and cyber criminals that may seek to exploit UK organisations and Infrastructure to further their own agenda and prosperity. Campaigns can be persistent, including espionage, intellectual property theft or extortion by ransoming data, or through malware. [4]

Hazards

There are various *natural* hazards (e.g. flooding, severe weather and storms) that can also disrupt the day-to-day functioning of the UK's National Infrastructure. Disruption to National Infrastructure can also be caused by public disorder and societal pressures such as staff absence due to widespread influenza or industrial action leading to temporary closures, reduced services, or services continuing but at reduced capacity.

With the continual diversification and evolution of threats and hazards it's important to build the capability of the UK's Infrastructure to withstand and recover from a range of possible events.

[3] https://www.cpni.gov.uk/national-security-threats
[4] https://www.ncsc.gov.uk/news/2017-annual-review

Our Security & Resilience Approach

Government's core objective includes reducing CNI's vulnerability to threats and hazards and improving resilience, by strengthening the ability of CNI to withstand and recover from disruption. Its approach to security and resilience focuses on Resistance, Reliability, Redundancy, and Response & Recovery.

Figure 1: The components of Infrastructure resilience

- **Resistance:** Concerns direct physical protection (e.g. the erection of flood defences). Resistance is ensured by preventing damage or disruption through the protection of Infrastructure against threats and hazards. This includes reducing vulnerability through physical, personnel and cyber security measures.

- **Reliability:** The capability of Infrastructure to maintain operations under a range of conditions to mitigate damage from an event (e.g. by ensuring that electrical cabling is able to operate in extremes of heat and cold).

- **Redundancy:** The adaptability of an asset or network to ensure the availability of backup installations, systems or processes or spare capacity (e.g. back-up data centres).

- **Response and Recovery:** An organisation's ability to rapidly and effectively respond to and recover from disruptive events.

Roles and Responsibilities

A wide range of organisations are responsible for critical sectors' security and resilience, including the owners and operators, emergency services and local and central Government.

Infrastructure owners and operators

Day-to-day operating of our National Infrastructure is the responsibility of the owners and operators. They carry out risk assessments at the asset level and make calculated decisions on maintenance, training and investment to improve organisational and asset-level security and resilience.

Local authorities and emergency services

In accordance with the Civil Contingencies Act 2004, local authorities and emergency services are required to identify and assess the likelihood and impact of potential emergencies (including Infrastructure emergencies) that could affect members of the public within their areas of jurisdiction. They are also required to develop emergency response plans to address those risks.

Government Agencies

Several agencies provide central government, regulators and Infrastructure owners and operators with advice on Infrastructure risks and mitigation. For example, the Centre for the Protection of National Infrastructure (CPNI) provides protective security advice to businesses and organisations across the UK's National Infrastructure. They also provide integrated advice on physical and personnel security, aimed at minimising risk and reducing our vulnerability to terrorism, espionage, and other national security threats.

The National Cyber Security Centre (NCSC) was established in 2016 as part of the Government Communications Headquarters (GCHQ) and brings together cyber expertise from a wide range of previously disparate cyber organisations. The Centre's main purpose is to reduce the cyber security risk to the UK, working with businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management, underpinned by world class research and innovation.

Regulators

Regulators support Lead Government Departments by ensuring relevant legislation and regulation are observed, for example as part of sites' licence conditions. To build resilience, some regulators can intervene and require organisations to meet particular security and resilience obligations or standards as conditions for their continued operation.

Lead Government Departments

Lead Government Departments are responsible for sector-level security and resilience policy development (including legislation). They produce the Sector Security and Resilience Plans (SSRPs), which set out each Department's understanding of the risks to their sectors and the key activities they will undertake to address those risks during the year ahead. The 2017 SSRPs are summarised in the following section of this document.

Public Summaries

This section of the document sets out the public summaries of the 2017-18 Sector Security and Resilience Plans (SSRPs). The table below shows which Lead Government Department is responsible for producing each SSRP.

Sector	Sector Resilience Lead [5]
Chemicals	Department for Business, Energy and Industrial Strategy
Civil Nuclear	Department for Business, Energy and Industrial Strategy
Communications	Department for Culture, Media and Sport
Defence	Ministry of Defence
Emergency Services	Department of Health
	Department for Transport
	Home Office
Energy	Department for Business, Energy and Industrial Strategy
Finance	HM Treasury
Food	Department for Environment, Food and Rural Affairs
Government	Cabinet Office
Health	Department of Health
Space	UK Space Agency
Transport	Department for Transport
Water	Department for Environment, Food and Rural Affairs

[5] 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 2017 Sector Security and Resilience Plans covered the entirety of the UK.

Chemicals Sector

Department for Business, Energy and Industrial Strategy

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 designated Chemicals as a critical sector in 2015.

Assessment of Existing Resilience

Resilience in the Chemicals sector is not specifically mandated by regulation, but the requirement for site owners to comply with safety and environmental legislation or conventions promotes a strong safety culture; for example:

- Sites producing certain quantities of particular chemicals relevant to the Chemical Weapons Convention (CWC) are subject to data monitoring, licensing and national/international inspection.
- Sites subject to COMAH (Control of Major Accident Hazards) 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[6] which do occur.
- By working with local emergency planners and responders to prepare suitable emergency plans.

To support site protection and incident response at the local level, 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. Building resilience in the sector has focused on preventing or minimising casualties following a chemical release and preventing their use in explosive devices.

Building Resilience

Work continues with stakeholders – site owners, sector organisations and across Government – to encourage and promote resilience. Work will continue to encourage relevant sites to consider their resilience to major risks and to develop mitigating measures so that the impacts on the public and essential services will be minimized.

[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

Civil Nuclear Sector

Department for Business, Energy and Industrial Strategy

The Civil 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 responsible LGD, 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:** The UK's obligations concerning the reporting and/or publication of safeguards related information were met. Euratom[7] and IAEA[8] reports of 2014 and 2015 concluded there had been no diversion of civil nuclear material from peaceful use in the UK.

- 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;
- Ensures effective communications with local, national, and international audiences.

Building Resilience

The Department for Business, Energy and Industrial Strategy (and previously 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.

[7] European Atomic Energy Committee
[8] https://www.iaea.org/

Communications Sector

Department for Culture, Media and Sport

The Communications sector comprises telecommunications, internet, postal services and broadcast. The sector has invested proportionately in each of its sub-sector's 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 Critical 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 protection of key sites and networks from natural hazards as well as physical and electronic security threats.

The sector has invested proportionately in its resilience. 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.

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/internet. 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 Sector

Ministry of Defence

Defence was officially designated as a critical sector in 2014, and was previously part of the Government sector.

The Ministry of Defence (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's Security Framework, and works with other departments to maximise the security of its sites, personnel and equipment. MOD has sites across the UK and is exposed to a range of local weather and environmental hazards.

Building Resilience

The Strategic Defence and Security Review reinforced MOD's role in supporting the UK's resilience.

Head Office will continue to fulfil a coordinating function to develop their understanding of the resilience requirements of their business and critical functions.

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

Emergency Services Sector

Home Office, Department for Transport & Department for Health

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

Assessment of Existing Resilience

Emergency Services are subject to the full set of civil protection duties under the Civil Contingencies Act (2004). This includes the requirement to assess the risks and put in place emergency and business continuity plans.

The major risks to the sector are loss of communications and loss of power. 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, as well as local solutions. To support emergency response during periods of disruption from major 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[9];
- 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 Her Majesty's Inspectorate of Constabulary-led tri-service team; 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 the Centre for the Protection of National Infrastructure (CPNI) was initiated in 2013.

[9] 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 Sector

Department for Business, Energy and Industrial Strategy

The Energy 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. It is not cost effective or feasible to mitigate every risk. However, Government, regulators, and the supply industry work together to ensure risks to supply are appropriately managed. 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 ensures 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: Ensuring an acceptable and affordable level of Black Start service. Black Start is the term given to the restoration plans developed by National Grid to restore the National Electricity Transmission System in the event of its total failure.
- Energy Networks: Assessment of the risk posed by 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 Sector

Her Majesty's Treasury

Over the past year, the Finance sector has continued to make 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 increasingly complex and sophisticated 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 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 completing the first phase of the Bank of England's CBEST cyber vulnerability testing programme.
- HM Treasury, the Bank of England, and the Financial Conduct Authority have refined and tested their own response frameworks to reflect the creation of the National Cyber Security Centre, as well as lessons learned from recent incidents. This has included working with the Finance sector to test collective response to operational disruption.

Building Resilience

Over the next year, HM Treasury will:

- Work with the Bank of England and the Financial Conduct Authority, drawing on the expertise of the National Cyber Security Centre to improve the resilience of the finance sector.
- Continue to test the resilience of the sector, and refine and improve its response frameworks.
- Further analyse the potential impacts on the Finance sector from severe space weather, as well as disruption to other essential services such as communications and power networks.
- Maintain strong links with international partners, including through the G7 Cyber Expert Group reporting to G7 Ministers and Central Bank Governors.
- Continue to work closely with the Finance sector, including through the senior Cross Market Operational Resilience Group (CMORG), chaired by the Bank of England, and the FCA's new Cyber Coordination Groups for specific sub-sectors in financial services.

Food Sector

Department for Environment, Food and Rural Affairs

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 its 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.

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 including by updating PAS96.

Government Sector

Cabinet Office

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 to the sector. A broad range of measures are in place which are kept under regular review to counter 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 to the sector include malicious cyber activity, acts of terrorism, and other criminal activity, as well as technical failures. The breadth of these concerns requires a range of security and resilience measures to be adopted by the sector which calls for greater education, training and exercising.
- 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 already benefitted from the expertise in the National Cyber Security Centre.
- Government is currently transforming how security is delivered within departments to ensure a robust security culture which is able to respond to both current and future threats. Improvements have already been made by introducing clustered shared service models which provide a consistent and high standard of expertise across government.

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. Improvements in working with the commercial sector will help to deliver increased security assurance from suppliers. Where appropriate, Cabinet Office continues to engage with Devolved Administrations to deliver mutually supportive programmes and ensure that resources can be prioritised and expertise shared.

Health Sector

Department of Health

The Department of Health (DH) is the Lead Government Department responsible for Health sector CNI and for managing any risks.

Assessment of Existing Resilience

The NHS and Public Health England (PHE) have good levels of resilience and an ability to divert resources from non-essential services to life-saving treatment in an emergency. 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 a response, the social care sector is more challenging to understand. Continuous 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 continued to ensure that they had 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 will be working across the health sector to consider resilience to prolonged electricity supply disruption and fuel shortages, as well as the recommendations from 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 NHSBT will continue to progress work on the findings of the Mass Casualties National Capabilities Risk Assessment (NCRA).

Transport Sector

Department for Transport

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 ensures that proportionate and cost-effective mitigations are in place.

The Department works closely with the British Transport Police and Maritime and Coastguard Agency to deliver effective emergency response to, and mitigation against, security hazards.

As part of its regular resilience work, DfT:

- Maintains collaborative relationships with the transport industry.
- Has a specific engagement programme with industry on winter weather resilience.
- Delivers targeted research programmes to provide evidence supporting policy development for secure and resilient transport.

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, technological solutions, and the interconnected nature of transport networks all enhance the resilience of the sector.

Building Resilience

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

- **Security:** DfT 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:** DfT works with the intelligence community, other departments, local responders and industry, and has well exercised internal response procedures.

- **Cyber incident:** 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:** As part of the 2016 National Flood Resilience Review, The Department is working to identify local road networks in England that are at risk of flooding, and assess the impact of un-accessible roads and bridges on communities. Network Rail is developing route resilience plans to identify areas vulnerable to flooding.

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

- **Severe space weather:** DfT is 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.

Water Sector

Department for Environment, Food and Rural Affairs

The Department for Environment, Food and Rural Affairs is the Lead Government Department responsible for Water sector CNI and for managing any risks.

An all risks regulatory framework, effective mutual aid arrangements 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.
- Emergency response is bolstered by industry-wide and local mutual aid agreements to enable the sharing of resources between companies.
- All companies maintain statutory plans to minimise the impact of a drought.

Further Information

Links to some additional information relevant to the SSRPs are provided below.

- The National Security Strategy and Strategic Defence and Security Review (NSS & SDSR) describes the UKs national security objectives and interests and how they will be delivered.
- The National Risks Register (NRR) describes significant risks, including malicious threats and natural hazards that could affect the UK.
- The National Cyber Security Strategy 2016-2021 sets out HMG's strategy for tacking cyber security risks.
- Further information on cyber security is available on the National Cyber Security Centre's website.
- Further information on protective security is available on the Centre for the Protection of National Infrastructure's website.